Riigi Infosüsteemi Amet

# Küberturvalisuse aastaraamat 2021

Riigi Infosüsteemi Amet

# Küberturvalisuse aastaraamat 2021

# Sisukord

## EESSÕNA



## 2020. AASTA ÜLEVAADE



## TURVALISEM KÜBERRUUM




# (Digi)kriisi lahendamine eeldab selget juhtimist

Koroonakriis kasvatab meie sõltuvust digitaalsetest lahendustest veelgi. See tähendab, et ka e-riiki ja selle turvalisusesse tuleb panustada rohkem, kirjutab riigi infosüsteemi ameti peadirektor **Margus Noormaa**.

2020 oli enneolematu aasta. COVID-19 epideemia tegi ja teeb siiani suurt laastamistööd ning üleilmse kriisi tagajärgedega tuleb õppida elama. Kaugtöö jääb üheks töötamise vormiks, füüsilisi kokkupuuteid mõne teenuse tarbimiseks on vaja järjest vähem.

Igasugune kriisiaeg või uus olukord soosib arengut, ka negatiivset. Näost näkku kohtumisel ei saa kurjategijad vahele imbuda, digitehingule aga saavad, kui seda ei tehta targalt ja turvaliselt. Pole juhus, et just koroona-aastal sagenesid õngitsuskampaaniad, mille kaudu üritasid kelmid pääseda ligi inimeste andmetele ja rahale ning aina sagedamini pidid ettevõtted tegelema küberrünnaku alla sattunud veebilehtede, sh informatsiooni taastamisega.

## Turvalisus vajab rohkem tähelepanu

Lugusid, millest õppida, ei tule kaugelt otsida. Eelmisel sügisel otsisid kurjategijad veebilehtede nõrkusi. Nende sihitud ja konkreetne töö kandis vilja – nad pääsesid ligi ka kolme Eesti ministeeriumi serveritele ning kätte saadi tundlikke terviseandmeid. Ministeeriumide ja RIA, täpsemalt CERT-EE kiire reageerimine päästis hullemast, aga sai selgeks, et meie e-riigi turvalisusesse tuleb kriitilisemalt suhtuda.

On palju parem, kui viga avastatakse tehnoülevaatusel, mitte autoroolis kiirusel 90 km/h. Kui siis pidurid üles ütlevad, terendab silmapiiril raske õnnetus. Teeme RIAs omalt poolt kõik, et asutused suhtuksid enda lahendustesse täie tähelepanuga ning hoiaksid süsteemid parimas korras.

Kuigi oleme oma digiriiki ehitanud juba üle 20 aasta ning selles vallas kindlasti muu maailmaga võrreldes eelisseisus, ei tööta masinavärk sugugi veatult. Rohkem on vaja erinevate lahenduste koostoimet, andmete paremat kasutamist ja selgemat vaadet, mida meil siis ikkagi oleks vaja teha.

**MARGUS NOORMAA**
riigi infosüsteemi ameti peadirektor

Siiani on Eesti digiedu taga olnud IT-sektor ja selle kogukonna aktivistid. On viimane aeg, et vedaja rolli võtab nüüd äripool ehk riiklik tellija, kes ütleb, mida ja mille jaoks, millises järjekorras ja mis prioriteetsusega tuleb riigis teha. Ning ka rahastab seda vastavalt. Siis on lootust, et uute kriiside ajal oleme paremini valmis, vähemalt digitaalsete lahendustega.

## Igaüks saab panustada

Küberturvalisusega on lihtsam – siin saab igaüks kaasa lüüa. Kehtib nõrgima lüli põhimõte, st et nii tugevad kui on meie turvalisuse ahela kõige nõrgemad lülid, nii turvaline on ka meie keskkond. Mulle tundub, et turvalisuse küsimus pole enam kellelegi arusaamatu, selle vajalikkust mõistetakse ja osatakse nõu küsida. Siin on RIA hea meelega abiks.

Toon mõned näited. RIA CERT-EE pakub erinevaid tasuta tööriistu, mille abil leida kriitilisi vigu ning need enne kurjategijate huviorbiiti sattumist parandada. Pakume neid kõigile soovijatele. Sarnaseks abivahendiks on ka RIA loodud värske Eesti infoturbestandard – see annab asutustele kätte raamistiku, kuidas korraldada oma infoturvet nii, et andmekogud on kaitstud ja töötavad tõrgeteta.

> Mulle tundub, et turvalisuse küsimus pole enam kellelegi arusaamatu, selle vajalikkust mõistetakse ja osatakse nõu küsida. Siin on RIA hea meelega abiks.

Tervishoiuvaldkond, mis on kriisi tõttu niigi tohutu surve all, pole saanud rakendada häid e-lahendusi, mis toetaks arste ja õdesid nende igapäevatöös. Neid lahendusi pole, sest varem, kriisivälisel ajal, ei peetud neid nii oluliseks. Kriis annab meditsiinivaldkonna IT-le eeldatavasti korraliku hoo sisse ja ennaktempos valmivad lahendused, mis muidu pidanuks veel kümme aastat ootama. Kas oleksime saanud seda ette näha ning minevikus paremini planeerida ja arendada? Jah ja ei.

Kas me oleme piisavalt väärtustanud IT rolli oma äri korraldamisel? Kas me oleme piisavalt pühendanud tähelepanu infoturbeküsimustele? Kuidas saaks korraldada oma inimeste tööd selliselt, et kõik igavad rutiinid lükkaks tehnoloogia kanda ja võimaldaks inimestel pühenduda oma tööle, et nad saaksid ravida, juhtida, ehitada, kaitsta ja õpetada? Tasub võtta aega ja nendele küsimustele mõelda. Pikalt ja põhjalikult. Siis on lootust, et järgmisesse kriisi minnes on vähem digipaanikat ja rohkem koostegemist.

# Olukorrast küberruumis: rekordarv õngitsusi

2020. aastat küberruumis jäävad meenutama rekordarv õngitsusi, salakaval pahavara Emotet ja ummistusründed.

Jaanuari esimestel minutitel üksteisele head soovides ei osanud keegi aimata, et 2020. aasta kujuneb eelnevatest nii erinevaks. Hiinast alguse saanud koroonaviirus COVID-19 jõudis veebruaris Eestisse ja 12. märtsil kuulutas valitsus selle leviku piiramiseks välja eriolukorra.

Vaid mõne päeva jooksul läksid ettevõtted ja asutused üle kaugtööle ning koolid distantsõppele. Digiriik pandi proovile: e-teenuste kasutamine kasvas hüppeliselt nii õppimisel, töötamisel, ostlemisel, meelelahutamisel kui info hankimisel. Elektroonne õppeinfosüsteem eKool ei pidanud distantsõppe esimesel päeval järsult kasvanud koormusele vastu, kuid selle töö taastus ressursside lisamise järel.

Kiiruga võeti kasutusele uusi digitaalseid teenuseid ja loodi uusi kontosid, kasutades pahatihti vanu paroole. Kõik eelnev ja koroonakriisiga kaasnenud ärevus lõid soodsa pinnase küberintsidentide arvu järsuks tõusuks. Ehkki mõne pettuse- või rünnakuliigi puhul nägime kasvu, võime aastale tagasi vaadates öelda, et läbisime „stressitesti“ suhteliselt edukalt.

## Pangakontode õngitsused

Üks neist küberintsidentide liikidest, mille hulk eelmisel aastal kasvas, olid õngitsuslehed. Mullu registreerisime neid viiendiku võrra rohkem ja need moodustasid üle veerandi kõikidest mõjuga intsidentidest.

Õngitsused võib laias laastus jaotada kaheks: pangakontode ja meilikontode õngitsusteks. 2019. aastal alguse saanud petukirjade laine, millega õngitseti internetipanka sisselogimiseks ja maksete tegemiseks vajalikke paroole ja PIN-koode, jätkus eelmisel aastal. Saime teateid 41 pangaandmeid õngitseva petulehe kohta.

Enamasti saatsid petturid masspostitusega e-kirju, milles esinesid panga töötajana ja palusid kirjas oleva lingi kaudu sisse logida lehel, mis oli äravahetamiseni sarnane õige internetipanga lehega. Samal ajal kui ohver sisestas libalehel oma kontoandmeid, tegi pet-

tur sedasama ehtsas internetipangas, kasutades andmeid, mida ohver võltslehele kirjutas. Kui pahaaimamatu kasutaja sisestas ka nutiseadmes või telefonis Smart-ID või mobiil-ID PIN-koodi, pääseski kurjategija pangakontole ja kandis seal oleva raha enda kontrolli all olevale kontole.

RIA intsidentide käsitlemise osakond CERT-EE teavitab sellistel puhkudel veebimajutajat, kelle serveris õngitsusleht asub, ja palub selle eemaldada, kuid tõhusam rohi niisuguste pettuste vastu on teadlik ja tähelepanelik arvutikasutaja. Lähemal uurimisel märkaks kirja saaja, et saatja ja õngitsuslehe aadress on tavapärasest erinevad ega pruugi kuuluda pangale. Internetipanka sisenedes tuleks selle aadress ise veebilehitseja aadressiribale kirjutada, mitte avada kahtlastes meilides olevaid linke.

Kolmandas kvartalis saime teavitusi seesugustest pettustest peaaegu iga nädal, kuid 28. septembril juhtus midagi, mis neile ajutiselt pidurit tõmbas. Rahvusvahelise politseikoostöö raames peeti Rumeenias kinni kolm meest, keda kahtlustatakse kirjeldatud õngitsuste läbiviimises. Eestis jõudsid nende saadetud õngitsuskirjad kuni 100 000 inimeseni, kellest vähemalt 400 kontole õnnestus kurjategijatel ligi pääseda.

> Kokku üritati kannatanute kontodelt ära kanda ligi 150 000 eurot.

Kokku üritati kannatanute kontodelt ära kanda ligi 150 000 eurot. Kõik katsed ei õnnestunud: mõnel juhul said inimesed ise aru, et tegemist on kelmusega ega kinnitanud

tehingut PIN2 parooliga, teistel puhkudel blokeerisid kahtlase makse pangad. Politseile teadaolevalt õnnestus kurjategijatel raha varastada siiski ligi 40 inimese kontolt ning kahjusumma moodustas üle 100 000 euro.

Pärast Bukarestis toimunud vahistamist saabus pangaõngitsuste rindele kuu aega kestnud vaikus, kuid oktoobri lõpus hakkasid need taas levima.

### Meilikontode õngitsused võivad viia arvepettusteni

Kui pangaõngitsuste tekitatud kahju on kohe näha, siis meilikontode õngitsuste puhul võivad tagajärjed ilmneda tükk aega hiljem.

Ohvri e-posti kontole ligipääsu saanud kurjategija võib kuude kaupa jälgida tema kirjavahetust kolleegide ja koostööpartneritega ning koguda väärtuslikku teavet järgmise kuritöö, näiteks arvepettuse läbiviimiseks. Sobival hetkel sekkub pettur kirjavahetusse, esineb kaaperdatud meilikonto omanikuna ning teatab, et ettevõtte pangakonto on muutunud, ja palub lisatud arve tasuda uuele kontole. Kui arve saaja seda infot üle ei kontrolli – näiteks helistades koostööpartnerile – ja kannab arvel märgitud summa uuele kontole, võib see raha olla igaveseks kadunud.

Kui 2019. aastal oli meile teadaolevalt suurim summa, mis pettuse tõttu valele pangakontole kanti, 112 000 eurot (õnneks saadi see tänu pankadevahelisele koostööle tagasi), siis mullu oli suurim ühekordne kahju 41 000 eurot, mille ühe Viljandi ettevõtte koostööpartner petturite kontole kandis. Meile antakse aastas teada kümnetest niisugustest pettustest, kuid nende tegelik hulk ja põhjustatud kahju on kindlasti oluliselt suurem. Pikemalt kirjutame pettustest lk 20.

Kui ohver kasutab sama kasutajanime ja parooli mitmes teenuses, on võimalik kahju suurem, kuna pettur saab sama võtmega avada uksed ka ohvri teistele kontodele. Seepärast soovitamegi kasutada unikaalseid paroole ja kus vähegi võimalik, ka mitmeastmelist autentimist.

### Väljapressimistega ummistusründed on tagasi

2020 oli aasta, mil hajusad teenusetõkestusründed (DDoS) andsid end igapäevaelus taas tunda: kasvas nii nende hulk kui ka mõju. Väiksemate rünnete ja tõhusamate vastumeetmete korral piirdus kahju sellega, et ettevõtte koduleht toimis tavapärasest aeglasemalt või polnud mõne minuti jooksul kättesaadav, ent paraku oli ka tõsisemate tagajärgedega DDoSe, mis mõjutasid suuremat osa ühiskonnast.

Sügisel rünnati Eestis tegutsevaid kommertspankasid. Suurima mõjuga DDoSi puhul ei saanud paari tunni jooksul kasutada makseterminale: ära jäi või lükkus edasi miljonite eurode väärtuses tehinguid. Samal ajal jäid paljude klientide jaoks tundideks kättesaamatuks ka internetipank ja mobiiliäpp.

Suur osa ummistusrünnetest oli sama käekirjaga: ettevõttesse saadeti väljapressimiskiri, millele järgnes näidisrünnak ja ähvardus, et (krüpto)raha maksmata jätmisel rünnatakse uuesti ning siis suurema mahuga.

Põhjalikuma ülevaate ummistusrünnetest leiad lk 16.

### Turvanõrkused, mis võinuks kalliks maksma minna

2020. aastal tuvastas CERT-EE küberruumi seire või mõne intsidendi lahendamise käigus

2020. AASTA ARVUDES

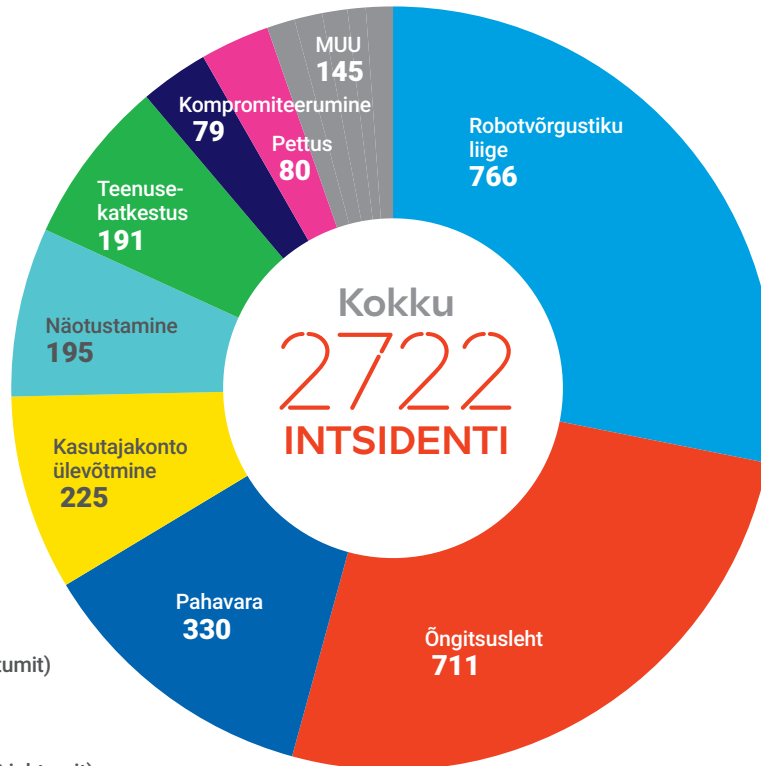
2020. aastal laekus RIA intsidentide käsitlemise osakonda CERT-EE

22 896 PÖÖRDUMIST

See on keskmiselt

63 PÖÖRDUMIST PÄEVAS

## Registreeritud intsidentide hulk ja osakaal 2020. a




„MUU" alla kuuluvad
- Lunavara (32 juhtumit)
- Teenustõkestusrünne (32 juhtumit)
- Juhtserver (29 juhtumit)
- Andmeleke (21 juhtumit)
- SEO-spämm (18 juhtumit)
- Krüptoraha kaevandamine (13 juhtumit)

mitmeid seni teadmata turvanõrkusi. Teavitasime toote omanikku või teenusepakkujat ja puudused eemaldati enne, kui suurem kahju jõudis sündida.

Juulis tuvastas CERT-EE ligi paarkümmend turvanõrkustega veebilehte, mis ei kontrollinud ID-kaardiga autentimisel, kas kaardi sertifikaat on kehtiv või mitte. Kahel juhul puudus ka kontroll, kas sertifikaat on SK ID Solutionsi poolt allkirjastatud. See tähendab, et kasutaja saanuks nendesse teenustesse logimisel ise sertifikaadi allkirjastada ning logida keskkonda ükskõik kelle nime ja isikukoodiga. Teavitasime veebilehtede omanikke leitud nõrkustest ja palusime need parandada.

Detsembris tuli see teema uuesti lauale, kui avastasime kiirlaenu pakkuva ettevõtte veebilehel sarnase nõrkuse. Selle kaudu saanuks võtta võõra inimese nimel laenu. Teavitasime ettevõtet ja aitasime puuduse kõrvaldada.

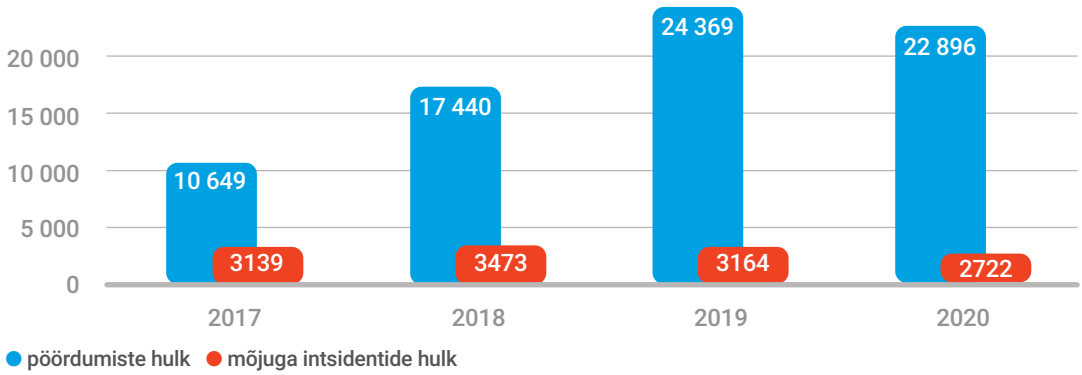
Suurt osa küberintsidentidest aitab ära hoida teadlik ja ettevaatlik arvutikasutaja, kuid sedalaadi nõrkuse puhul on vastutus teenusepakkujal. Korrektselt seadistatud veebileht ei jäta ründajale võimalust kasutajaid selliselt kuritarvitada. Kõik riiklikke autentimisteenu-

Neist olid **2722** **MÕJUGA INTSIDENDID,** mille tõttu olid häiritud teabe või süsteemide konfidentsiaalsus, terviklus või kättesaadavus.

Saime teateid **711** **ÕNGITSUSLEHEST.** Enim peavalu valmistasid pankade veebilehti matkivad õngitsuslehed.

Meid teavitati **225** **KASUTAJAKONTO ÜLEVÕTMISEST.** Enamasti langesid ründajate küüsi e-posti- ja sotsiaalmeediakontod.

## RIA poole pöördumiste ja mõjuga intsidentide hulk




seid kasutavad ettevõtted peaksid üle vaatama veebiserveri seadistuse ning veenduma, et lähtutakse parimatest praktikatest. Veebiserverite seadistamise uuendatud juhendid leiad portaalist www.id.ee.

Aasta lõpus teatasid Tartu Ülikooli teadlased, et avastasid nõrkuse ID-kaardi brauserilaienduses, mida kasutatakse ID-kaardiga digiallkirjade andmiseks. Kurjategija saanuks seda nõrkust ära kasutada, kui ta kas võtnuks üle või omanuks veebilehte, kus saab ID-kaardiga autentida. Kui kasutaja loginuks ründaja kontrolli all olnud lehel ID-kaardiga, saanuks ründaja kasutada autentimistoimingu infot, et kasutaja nimel sisse logida mõnda teise e-teenusesse.

Ehkki selle nõrkuse ärakasutamine oli keeruline ja meile teadaolevalt pole seda kordagi tehtud, võtame selliseid teateid alati täie tõsidusega. Koostöös partneritega parandasime selle haavatavuse ja tänavu jaanuaris andsime välja paigatud ID-tarkvara.

### Salakaval Emotet jõudis Eestisse

Eelmise aasta suvel jõudis taas kord Eestisse üheks ohtlikumaks ja salakavalamaks pahavaravõrgustikuks peetud Emotet. Tegu oli troojalasega, mis tekitas nakatunud süsteemidesse justkui tagaukse. Selle kaudu said teised küberkurjategijad paigaldada ohvri arvutisse muu pahavara, mille kaudu varastada andmeid või viia läbi teisi rünnakuid.

Emotet levis enamasti e-kirjadele lisatud failide kaudu. Tuttavalt inimeselt saabus senise kirjavahetuse jätkuna kiri, mille sisuks oli näiteks „Manuses on uus arve“ või „Please confirm“ ja kaasas näiliselt tavaline Wordi või Exceli fail. Selle avamisel teatas programm, et makrosisu on keelatud, ja palus selle lubamiseks teha veel üks hiireklõps nupul „Enable Content“ või „Luba sisu“. Seda tehes andis pahaaimamatu kasutaja käsu paigaldada oma arvutisse Emoteti pahavara.

> Õnneks saame Emotetist kirjutada minevikuvormis.

Saime eelmisel aastal teateid sadadest Emotetiga nakatunud seadmetes Eestis. Neid oli peaaegu igast valdkonnast: majutusettevõtetest tervishoiusektorini, riigi- ja kohaliku omavalitsuse asutustest projekteerimisfirmadeni.

Õnneks saame Emotetist kirjutada minevikuvormis. 2021. aasta alguses võeti rahvusvahelise politseioperatsiooni käigus maha Emoteti taristu, kuhu kuulus sadu servereid üle maailma. Pärast seda pole värskeid nakatumisi tuvastatud ja ka varem nakatunud seadmete omanikud ei pea enam Emoteti pärast muretsema.

### Teenusekatkestused mõjutasid meid kõiki

2020. aastal saime teateid 170 teenusekatkestusest. Enamasti oli nende taga inimlik eksimus või seadistusviga, aga mõnel juhul katkesid e-teenused ka pahatahtliku rünnaku tõttu. Väga ränkade tagajärgedega teenusekatkestusi õnneks polnud.

Mitmel korral oli tõrkeid avalikule sektorile andmesideteenust pakkuva riigivõrgu töös. Näiteks 23. jaanuaril suunati plaanitud hooldustööde käigus riigivõrgu liiklus tagavaratrassile. See aga ei tulnud kasvanud koormusega toime, mistõttu oli andmesideühendus ligi 2,5 tunni jooksul häiritud kuni kolmandikul riigivõrgu klientidest.

Kuraditosinal korral katkesid haigekassa e-teenused, milles tuntumad on digiretsept ja kindlustatuse kontroll.

Enamik nii riigivõrgu kui ka haigekassa intsidentidest jäi aasta esimesse poolde, teisel poolaastal paranes nende töökindlus märgatavalt.

23. veebruaril polnud viie tunni jooksul kättesaadav Luminori internetipank ega mobiilirakendus. 8. oktoobril olid rohkem kui kolme tunni jooksul häiritud Swedbanki teenused: internetipank, mobiiliäpp ja kaardimaksed.

### Robotvõrgustikud tegutsevad endiselt

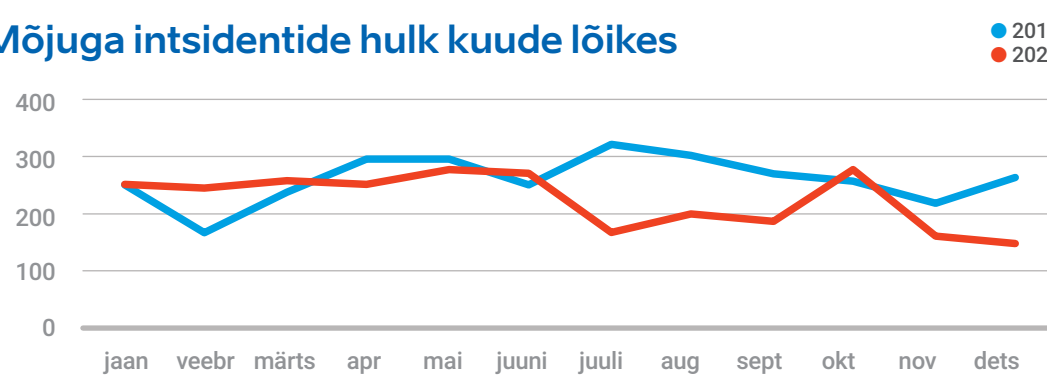
Juba aastaid moodustavad suurima osa CERT-EE registreeritud mõjuga intsidentidest robotvõrgustikega liitumised. See tähendab pahavaraga nakatunud seadmeid, mis on koondatud kurjategijate kontrolli all olevasse võrgustikku. Neid robotvõrgustikke (ingl k *botnet*), kuhu võib kuuluda kuni sadu tuhandeid arvuteid, kasutatakse küberrünnakute läbiviimiseks. Enamasti pole omanikul aimugi, et tema arvuti nakatati pahavaraga ja et see osales näiteks teenusetõkestusrünnakus mõne telekomifirma vastu.

Info nakatunumiste kohta saadame automaatteavitustena sideteenuse pakkujatele, kuid paraku ei jõua see sealt mõnikord edasi lõppklientideni, kelle seadmed pahavaraga nakatunud ja robotvõrgustikega liidetud. Selle kurvaks kinnituseks on intsidendid, mille põhjuseid uurides selgub, et neid saanuks ära hoida, kui sideteenuse pakkuja oleks CERT-EE saadetud hoiatusteated õigel ajal kliendini viinud.

Alates 2020. aasta juulist ei kajastu CERT-EE statistikas nakatumised Avalanche'i ja Necursiga, mis moodustasid ligi 95% meie poolt registreeritud robotvõrgustikega nakatumistest ja umbes 60% kõigist mõjuga intsidentidest. Avalanche peatati rahvusvahelise politseioperatsiooni tulemusel 2016. aasta detsembris, kuid nakatumised jätkusid hiljemgi. Necursi võrgustiku sai Microsoft enda kontrolli alla 2020. aasta märtsis.

Siiski on Eesti võrkudes endiselt suur hulk seadmeid, mis on nakatunud mõne aktiivse robotvõrgustikuga ja saadavad omaniku teadmata välja õngitsuskirju või osalevad ummistusrünnetes võib-olla isegi seadmeomaniku kodupanga vastu.

## Mõjuga intsidentide hulk kuude lõikes



# Aasta valusaim õppetund

2020. aasta suurima mõjuga küberintsident mõjutas riigisektorit: novembris avastasime kolm sarnase käekirjaga rünnakut majandus- ja kommunikatsiooniministeeriumi (MKM), sotsiaalministeeriumi (SoM) ja välisministeeriumi (VäM) serverite vastu.

Neid võrreldes ja analüüsides nägime, et ründaja kasutas kõigil kolmel juhul sarnast meetodit. Esmalt skanneeris ta veebiservereid. Kui avastas avalikuks unustatud tehnilise .git kataloogi kaudu turvanõrkused, laadis nende abil üles pahaloomulise ründekoodi. Olles serveritele ligi pääsenud, omastas ta ette jäänud andmed ning hakkas otsima, mida veel serveri kaudu kätte saab. Sellist käekirja oleme näinud ka pärast detsembris avalikustatud rünnakuid.

## Täiuslikku kaitset pole kellelgi

Riigi IT-taristu vastu tehtud edukad rünnakud näitavad, et keegi pole täielikult kaitstud. Eesti ministeeriumid kasutavad küll ühtseid välisveebe, kuid nende veebiserverid võivad majutada ka ükshaaval arendatud teisi lehe-

külgi. Samuti ei pruugi iga ministeerium või haldusala oma lehekülgi sarnaselt konfigureerida. On hulk väikeseid nüansse, mis erinevalt seadistades võivad avada ründevektori.

Nii oligi sügisese rünnaku suurim mõju MKMi haldusalas, kus veebiserveri ründamise järel õnnestus ründajatel pääseda edasi MKMi haldusala serveriteni, kust lekkis mitmesaja gigabaidi ulatuses andmeid.

Prominentseima andmelekke allikaks oli aga sotsiaalministeeriumi haldusala, kus kurjategijatel õnnestus veebiserverile ligi pääsedes jõuda COVID-19 pandeemiaga seotud, 9158 inimest puudutava informatsioonini. Ajutise lahendusena asus see kompromiteeritud veebiserveri andmebaasis.

Kõige kergemini pääses välisministeerium: nende kodulehelt ründaja edasi ei jõudnud ega saanud mitteavalikku infot.

### Valus õppetund

Kompromiteerimine ehk autoriseerimata ligipääsu omandamine andmetele või süsteemidele on väga suur oht. Ligipääsu saanud kurjategija võib andmeid muuta, kustutada või neid krüpteerida ning tekitada seeläbi meie igapäevases suhtluses e-riigiga tõsiseid katkestusi. Kujutage ette, mis juhtuks, kui ehitisregister oleks kättesaamatu terve päeva või lausa nädala.

Ründaja võib olla huvitatud ka rahast: müüa saadud andmed maha järgmistele ründajatele – kellelegi, kes käib lekkinud andmed ükshaaval läbi, otsides sealt võimalikke uusi sihtmärke.

Detsembris avalikustatud intsident andis RIA-le hea õppetunni, kuidas paremini kaitsta riigi IT-taristut. Iga asutus vastutab oma küberturvalisuse eest ise, kuid meile on seadusega antud ülesanne võimalike ohtude ilmnemisel teavitada neist kogu Eestit.

Seetõttu andsime erineva detailsusastmega soovitusi avaliku sektori infoturbejuhtidele, elutähtsate teenuste osutajatele ja laiemale küberturvalisuse kogukonnale. Need nõuanded pole kuigi keerukad ning pigem rõhutavad elementaarset IT-turvalisust: ära anna liiga palju infot, hoia ülevaadet oma varadest ja kasutajatest ning seira oma süsteeme.

Nüüd teame veel paremini, millist infot ründajad otsivad, kuidas nad seda kasutavad ja mida veel paremini seirata.

## CERT-EE soovitused infoturbejuhtidele

- **Uuenda:** veebide standardrakendustes on kriitilised nõrkused, mis on enamasti põhjustatud uuendamata tarkvarast.
- **Avalda vaid seda, mida vaja:** ära jäta koodi .git kataloogi kaudu avalikult kättesaadavaks. See võib anda ründajale vajalikku infot.
- **Oma ülevaadet kasutajatest ja anna muutmisõigus põhjendatult:** tihti on veebirakenduses ebavajalikke (tihti aegunud) administraatori õigustes kontosid, mille paroolid võivad olla lekkinud.
- **Eralda välisveeb sisemistest varadest:** veebiserverite puudulik või ebaturvaline eraldatus ülejäänud infosüsteemist ehk segmenteerimine annab ründajale võimaluse saada veebi kaudu ligi asutuse tundlikele infovaradele.
- **Hoia tundlikke andmeid hoolega:** veebiserveris ei tohi hoida andmeid, mis peavad olema korralikult kaitstud. Kui ründaja saab ligipääsu välisveebile, ei tohiks tal olla automaatselt ligipääsu tundlikele andmetele.

Nüüd teame veel paremini, millist infot ründajad otsivad, kuidas nad seda kasutavad ja mida veel paremini seirata.

# Ummistusrünnete arv kasvas, lisandusid väljapressimised

Möödunud aastal kasvas Eesti ettevõtteid ja asutusi tabanud teenusetõkestusrünnete arv poole võrra. Mitmed neist häirisid tuntavalt inimeste igapäevaelu.

Mullu anti meile teada 33 teenusetõkestusründest (inglise keeles *Denial of Service attack*, lühidalt DoS) ja nende mõju oli taas tuntav. Kord ei saanud poekassas tippajal kahe tunni jooksul pangakaardiga maksta, kahel korral olid tundide kaupa kättesaamatud ühe veebimajutaja klientide kodulehed, mitmel korral ei saanud inimesed teha oma tavapäraseid toiminguid internetipangas.

### Ei midagi enneolematut. Või siiski?

Uudse trendina võib välja tuua, et teenusetõkestusründeid hakati kasutama korduvateks väljapressimisteks. Möödunud sügisel said mitu Eesti ettevõtet kirja, kus ähvardati nende tegevus ummistusründega halvata, kui ettevõte ei maksa nõutud lunaraha. Kirjaga kaasnes näidisrünnak, mille ignoreerimisel ja teatud tähtajaks lunaraha mittetasumisel lubati naasta uue ja võimsama ründega.

Kurjategijad väitsid end olevat seotud mõne kurikuulsa küberrühmitusega nagu Fancy Bear, Cozy Bear või Armada Collective, lootes tuntud nime ja nende varem toimepandud kuritegude abil suurendada ähvarduse tõsiseltvõetavust.

Sihtmärgid polnud valitud juhuslikult: enamasti rünnati finants- või tehnoloogiasektori ettevõtteid. Nõutud lunaraha jäi vahemikku 0,5–10 bitcoini (10 000 – 400 000 eurot, sõltudes ka krüptoraha kursi muutustest).

Prognoosime teenusetõkestusrünnete mõju ja arvu kasvu ka 2021. aastal.

Praeguseks teame, et peaaegu kõikide sügisel rünnatud sihtmärkide vastu pandi selle aasta esimestel kuudel toime ka kordusrünnak. Kuna nimetatud sektorid on oma äri olemusest tulenevalt niikuinii keskmisest pare-

ma küberturbe tasemega ning tõhustasid esmaste intsidentide järel oma tehnilisi vastumeetmeid veelgi, läks ettevõtetel korda rünnakud mõne tunni jooksul tõrjuda ja normaalne töö taastada.

Teenuste katkemist või aeglust ei õnnestunud alati vältida, kõige pikemalt kestsid tõrked ligikaudu kuus tundi. Meie teada ei allunud aga ükski ettevõte kurjategijate nõudmistele ja loodetud lunaraha jäi vähemasti Eestist saamata.

### Kõigi rünnakute motivaator pole raha

Alati pole rünnakute motiiviks raha. Näiteks nägime möödunud aastal juhtumit, kus ühe Kesk-Eesti kooli veebipõhise õppetöö halvas sama kooli õpilane. Paraku mitte oma IT-alase nutikusega, vaid tellides teenust vastavalt lehelt. Eelmisesse aastasse jäi intsident, kus ühe ajalehe veebiversioon polnud ummistusründe tõttu suure osa päevast kättesaadav ning võimalik, et tegu oli kättemaksuaktsiooniga kriitilise artikli eest.

## Kuidas kaitsta end ummistusrünnete vastu?

- **Uuenda tarkvara**: nii rakenduste, võrguseadmete kui serverite tarkvaras võib olla turvanõrkuseid. Veendu, et kasutad tarkvara uusimat versiooni ning paigaldatud on kõik saadaolevad turvauuendused.
- **Võimalusel muuda veebilehed staatiliseks või kasuta veebipuhvrit**. Alternatiivne variant on hoida pidevalt uuendatuna dünaamilise lehe põhjal loodud staatilist versiooni, et ründe korral kiiresti staatilise peale ümber lülituda.
- **Kaitse veebivorme CAPTCHA abil,** ennetamaks või aeglustamaks veebilehtede vastu läbiviidavaid automatiseeritud ründeid.
- **Kasuta veebitulemüüri:** võimalusel kasuta pahaloomulist liiklust tekitavate IP-aadresside tuvastamiseks ja blokeerimiseks veebitulemüüri (Web Application Firewall ehk WAF).
- **Kasuta erinevate teenuste jaoks erinevaid servereid.** Näiteks ära käita nii oma meiliteenust kui ka veebiteenuseid samal füüsilisel serveril.
- **Võimalusel piira välismaist liiklust:** juhul kui teenused on mõeldud ainult Eesti kasutajatele, on võimalik (D)DoS ründe korral pöörduda oma internetiteenuse pakkuja poole ajutiseks liikluse piiramiseks teistest riikidest.

Möödunud aasta kevadel nägime ka ühte väiksemat lainet, kus sarnase käekirjaga lühiajalised ummistusründed pandi toime mitme Eesti jaoks olulise veebilehe vastu. Ehkki nende mõju oli väike, suhtume niisugustesse intsidentidesse tõsiselt – mõnikord võib esmase ründe eesmärk olla nõrkuste ja kasutatavate kaitsemeetmete väljaselgitamine, mille abil kavandada juba rohkem kahju põhjustavaid tegevusi.

Mida paremini on ettevõtted säärasteks rünnakuteks valmis, seda vähem tasuvaks muutub kurjategijatele nende ründamine. Siiski prognoosime teenusetõkestusrünnete mõju ja arvu kasvu ka 2021. aastal.

# Lunavararünnak: klassikat ja uusi tuuli

Käivitad pahaaimamatult arvuti ja avastad, et kõik sinu failid on krüpteeritud. Ekraanil aga kiri juhistega, kuhu ja mis ajaks teha krüptorahas ülekanne, et andmed tagasi saada. Just nii ebameeldivalt algas päev möödunud aastal ettevõtete või eraisikute jaoks meile teadaolevalt 32 korral.

Sihtmärkide seas oli väga erinevate elualade esindajaid: töötleva tööstuse ja kaubandusettevõtteid, haridusasutusi, arhitektuuribüroosid ning kaks perearstikeskust. Enamasti oli tegemist klassikalise lunavararünnakuga, millel on kolm sammu.

1. Ründaja paigaldab ohvri arvutisse või serverisse lunavara. Üha enam kasutatakse selleks ebaturvaliselt seadistatud kaugtöölauarakendust (Remote Desktop Protocol ehk RDP), kuid endiselt levib palju pahavara ka e-kirjaga saadetud failide ja linkide kaudu.
2. Lunavara krüpteerib kas osa arvutites või serverites olevatest failidest või kõvakettad tervikuna. Pärast seda ei saa ohver enam oma faile avada.
3. Ründaja nõuab failide taastamise ehk lahtikrüptimise eest lunaraha, enamasti mõnes krüptovaluutas nagu Bitcoin.

Eesti näidete puhul polnud lunavararünded sihitud spetsiaalselt ühe või teise valdkonna

suunas, piltlikult öeldes käivad kurjategijad pigem ringi ja katsuvad uksi ning kui peremees on olnud hooletu, ongi kahju kiire tulema. Selle suurus sõltub eelkõige varukoopiate olemasolust: kui need on tehtud, piisava regulaarsusega uuendatud ja talletatud ülejäänud infosüsteemist eraldi, on kaotus eelkõige taastamisele kuluv aeg.

Eelmise aasta juhtumite puhul nägime nii kiiret taastumist tänu eeskujulikule varundamisele kui ka seda, et kaotsi läks kogu raamatupidamine või viimaste kuude tehingute ja inventuuriandmed. Ehkki lunavararünnakud põhjustasid eelmisel aastal Eesti ettevõtetele nii ajakulu, tööprotsesside katkemist kui ka otsest majanduslikku kahju, võib kokkuvõtteks siiski tõdeda, et olukord võinuks olla hullem.

### Elu ja surma küsimus

Lunavararünnakud on maailmas tõusutrendis, seda nii arvuliselt kui ka tekitatud kahju poolest, mis võib ulatuda miljonitesse eurodesse. Läinud aastale andsid muu hulgas tooni lunavararünded haiglate ja muude tervishoiuasutuste vastu Prantsusmaal, USAs ja mujal maailmas, mille tagajärjed olid rahalisest kahjust tõsisemad: ohtu seati patsientide kiire ja asjakohane ravi.

Septembris toimus märgilise tähtsusega juhtum Saksamaal Düsseldorfis, kus lunavararünnak tõi kaasa inimohvri: haigla töö oli halvatud ning raskes seisus patsient suunati ümber, kuid ta suri teel teise haiglasse.

Lunavararünnakute kasvavat ja mitmepalgelisemaks muutuvat mõju näitab ka möödunud aastal tekkinud uus suund: sageli ei piirdu kurjategijad enam andmete krüpteerimisega, vaid ühtlasi varastavad need ja ähvardavad lunaraha maksmata jätmise korral avalikustada. Selline täiendav hirmufaktor võib olla mõjus, kui tegemist on näiteks delikaatsete andmete, hinnalise ärisaladuse või lihtsalt isikuandmetega, mille avalikuks tulemise korral ähvardavad andmete valdajat suured trahvid.

Soome ühiskonda raputas eelmisel sügisel juhtum, kus väljapressimiseks kasutatigi vaid varastatud andmeid (krüpteerimist ei toimunudki) ning neist osa jõudis tumeveebi. Tegu oli psühhoteraapiakeskuste klientide isikuandmete ja arstiga peetud vestlustega, mis on erakordselt tundlik teave. Väljapressimist võimaldanud andmelekke õigel ajal tähelepanuta jätnud ja selle tagajärjena usalduse kaotanud teraapiakeskuste kett on praeguseks pankrotis, tuhanded patsiendid aga juhtunust endiselt traumeeritud ja kindluseta, mis on nende isiklike haiguslugude edasine saatus.

## Kuidas kaitsta end lunavararünnaku eest?

1. Parim kaitse krüpteeriva lunavara vastu on läbimõeldud varundus. Vähemalt üks varukoopia peab asuma *offline*-režiimis, näiteks välisel kõvakettal.
2. Koolita töötajaid regulaarselt küberhügieenist, tuleta meelde, et tundmatutele linkidele ei tohi vajutada ega tundmatuid manuseid avada.
3. Rakenda pääsupoliitikat, millega tagatakse kasutajatele nende igapäevatööks minimaalsed õigused.
4. Vaata üle oma e-posti süsteemi turvapoliitikad ning veendu, et logimine on sisse lülitatud.
5. Kui kasutad kaugtöölauarakendust, muuda selle seadistus võimalikult turvaliseks.

Nii klassikaliste kui uudsemate lunavararünnakute eesmärk on sama – teenida kurjategijatele raha.

Nii klassikaliste kui uudsemate lunavararünnakute eesmärk on sama – teenida kurjategijatele raha. Mida rohkem edukaid rünnakuid ja nõudmistele allumisi, seda suurem on selle kuriteoliigi tasuvus ning seda motiveeritumad on kurjategijad oma meetodeid ja infrastruktuuri täiustama.

# Pettuseid oli rohkem, suuri kahjujuhtumeid vähem

Meile teada antud pettuste arv eelmisel aastal küll kasvas, kuid väga suurt rahalist kahju toonud juhtumeid oli varasemast vähem.

Kui kokkulepitud päeval palk töötaja kontole ei laekunud, hakkas ta uurima, milles asi. Saanud ühendust raamatupidajaga, kuulis ta suure üllatusena, et töötasu on üle kantud, aga uuele kontole, nagu ta ise olla soovinud.

Jälgi edasi ajades selgus, et paar nädalat varem oli end töötajana esitlenud pettur saatnud raamatupidajale e-kirja, kus palus seoses pangavahetusega kanda palk edaspidi uuele arveldusarvele. Näinud ekraanil kolleegi tuttavat nime, ei hakanud raamatupidaja saatja meiliaadressi (mis oli ilmselgelt kahtlane) üle kontrollima, vaid muutis raamatupidamisprogrammis kontonumbri ja kandis töötasu petturite kontrolli all olnud kontole.

Sedalaadi palgaandmete petuskeem hakkas maailmas levima 2019. aastal ja tekitas kahju ka mullu.

## Justkui ehtne arve, aga vale kontonumbriga

Lihtsamad arvepettused käivad kirjeldatud pangakonto pettustega sama skeemi järgi. Sageli ei ürita petturid enam ligi pääseda võõrastele meilivestlustele, vaid saadavad avalike andmete põhjal ettevõtetesse e-kirju ettepanekuga muuta edaspidiste arvelduste tarbeks arvelduskonto numbrit.

Mõnel juhul näevad petturid siiski rohkem vaeva. Saanud õngitsuse kaudu ligipääsu mõne töötaja meilikontole, võivad nad seal toimuvat kirjavahetust nädalate või kuude kaupa kannatlikult jälgida. Kui jutt läheb arve tasumisele, võtavad nad üht osapoolt matkides jutujärje üle, saadavad arve, mis on originaaliga äravahetamiseni sarnane – muudetud on vaid kontonumbrit.

Sageli avastatakse pettus alles siis, kui ülekannet ootav osapool hakkab uurima, miks nende saadetud arve on endiselt tasumata. Siis aga on kurjategijatele kantud raha väga keeruline tagasi saada.

## Haigla langes pettuse ohvriks

Eelmisel aastal andis arvepettusest teada Ida-Tallinna keskhaigla (ITKH). Seda eristas paljudest teistest asjaolu, et kurjategijad kasutasid pettuse ettevalmistamiseks ja läbiviimiseks avalikult kättesaadavat infot ühest ITKH

avalikust hankest. Nad kaaperdasid meilivestluse, vahetasid arvetel pangakonto numbrid ja petsid sel moel välja üle 10 000 euro.

Meile teadaolevalt oli mullu suurim ühekordne kahju üle 41 000 euro, mille ühe Viljandi ettevõtte partner petturite kontole kandis. Pettus ise käis tavapärase skeemi järgi: kurjategijad kompromiteerisid Viljandi ettevõtte töötaja konto ning jälgisid selle kaudu käivat kirjavahetust. Kui jutt läks arve tasumisele, võtsid sarnast meiliaadressi kasutanud petturid vestluse üle ja teatasid koostööpartnerile, et kuna Viljandi ettevõtte kodupank sattus uurimise alla, tuleks arve tasuda uuele kontole. Seda koostööpartner ka tegi.

Eelmisel aastal registreerisime kümneid sarnaseid pettuseid, kuid õnneks ei olnud kahjusummad enamasti väga suured. Selle aasta alguses aga toimus arvepettuse katse, mis õnnestumise korral purustanuks ligi 900 000 euroga kahjurekordeid. Tänu töötajate tähelepanelikkusele jäid maksed petturite kontole tegemata, aga see näitab, kui kõrge võib olla hooletuse hind.

## Kuidas kaitsta end palgakonto- ja arvepettuste eest?

- Kui saad partnerilt arve, kus on tavapärasest erinev kontonumber, küsi telefonitsi üle, kas ta on tõesti panka vahetanud.
- Kui töötaja palub kanda edaspidi palga uuele pangakontole, tee sama, mis eelmises punktis soovitatud.
- Isegi kui meili saatja nimi on tuttav, pööra tähelepanu saatja aadressile. Mõnikord kasutavad petturid visuaalset pettust, asendades nimes ühe tähe või muutes vaevumärgatavalt domeeni (ettevõte.ee *vs.* ettveõte.ee).
- Muuda meilivahetus turvalisemaks, kasutades SPF, DKIM ja DMARC protokolle. Täpsemad juhised leiad RIA kodulehelt.

Omal moel soodustas pettuseid ka koroonaviirus.

Omal moel soodustas pettuseid ka koroonaviirus: kuna rekordarv inimesi tegi kaugtööd ja varasemast suurem osa suhtlusest toimus üle interneti, oli kelmidel lihtsam tegutseda. Kui petturid saatsid end firma juhina esitledes raamatupidajale kirja, milles palusid teha kiiresti ülekanne tundmatule kontole, siis varem saanuks raamatupidaja küsida mõne meetri kaugusel istunud ülemuselt, kas tal on sellega tõsi taga ja nii pettusekatse paljastada. Kaugtööl olles peab selleks tegema mõned lisaliigutused, aga nagu ülal kirjeldatud juhtumid näitavad, tasub see väike vaev end kuhjaga ära.

# COVID-19 mõju Eesti küberruumile

Ehkki küberkurjategijad rakendasid COVID-19 pettustevankri ette, ei toonud koroonaviirus Eesti jaoks kaasa tavapärasest rohkem ega suurema mõjuga küberintsidente.

Eelmise aasta 8. märtsil saatis terviseamet eesti.ee postkastidesse e-kirja, milles jagas infot koroonaviiruse kohta. Vaid kaks päeva hiljem hakkasid levima terviseametit matkivad petukirjad, mis pakkusid samuti infot COVID-19 kohta, kuid mille tegelik eesmärk oli teine. Kirja lõpus oli link failile „Eeskiri.7z“. Sellel vajutamise järel avanes ekraanil pealtnäha tavaline ennetusplakat, aga taustal paigaldati ohvri arvutisse pahavara, mis varastas brauseritesse salvestatud salasõnad ja pangakaartide andmed.

## Leivanumbriks õngitsuskirjad

Petukirjade laineid, mis kasutasid ära COVID-19ga kaasnenud huvi ja ärevust, tuli veel. Osa

neist sisaldasid pahavara, osa aga võltsarveid kaitsemaskide eest, mida kirja saaja polnud tellinud. Kuid võrreldes mitme teise riigiga pääses Eesti küberruum suhteliselt kergelt: jäime puutumata osa Euroopa riike tabanud suunatud rünnetest meditsiinivaldkonna vastu ning ulatuslikku rahalist kahju põhjustanud COVID-19-teemalistest petuskeemidest.

Samuti ei toonud märkimisväärseid COVIDiga seotud arenguid viiruse sügisel alanud teine laine, kuigi mujal maailmas proovisid küberkurjategijad varastada vaktsiinide arendamisega seotud salastatud teavet.

### Suurima mõjuga „COVID-intsident" – isikuandmete leke

2020. aastal oli tõsiseim Eestit tabanud küberintsident majandus- ja kommunikatsiooniministeeriumi haldusalas toimunu (loe selle kohta lk 14). On põhjust arvata, et samad kurjategijad pääsesid novembri lõpus ligi ka sotsiaalministeeriumi haldusalas 9158 inimese informatsioonile, mis seotud koroonaviiruse levikuga. Ajutise lahendusena hoiti neid andmeid ühe veebiserveri andmebaasis. Ründaja juurdepääs sellele elimineeriti samal päeval ning terviseamet teavitas neid inimesi, kelle andmetele kurjategija ligi pääses.

## RIA toetab tervishoidu

RIA küberturvalisuse teenistuse kriitilise informatsiooni infrastruktuuri kaitse (KIIK) osakond toetab küberturbe küsimustes mitme eluala esindajaid. Nende hulgas on üheks olulisemaks meditsiinivaldkond, mis oli meie fookuses juba pandeemiaeelsetes plaanides.

Nimelt alustasime koolitustega perearstidele, kelle IT-süsteemid peavad 2022. aastast vastama küberturvalisuse seaduses kehtestatud nõuetele. Loomulikult on meditsiinivaldkonna peamine ülesanne eelkõige tervishoiuteenuste osutamine, kuid seejuures tuleb tähelepanu pöörata ka küberturvalisusele.

Märtsis ehk kohe COVID-19 Eestisse jõudes nõustasime perearstide seltsi, tervishoiutöötajaid ja haiglaid kaugtööle ülemineku, küberhügieeni reeglite ja digivõimekuse teemal. Aitasime hinnata arstidele kaugtööks vajaliku tarkvara turvalisust. Läbi aasta vahendasime infot potentsiaalsetest küberohtudest ning enda kaitsmise parimatest praktikatest.

ENISA üleeuroopaline meditsiinivaldkonda puudutav õppus CyberEurope jäi planeeritud ajal ära, kuid toimub 2021. aastal.

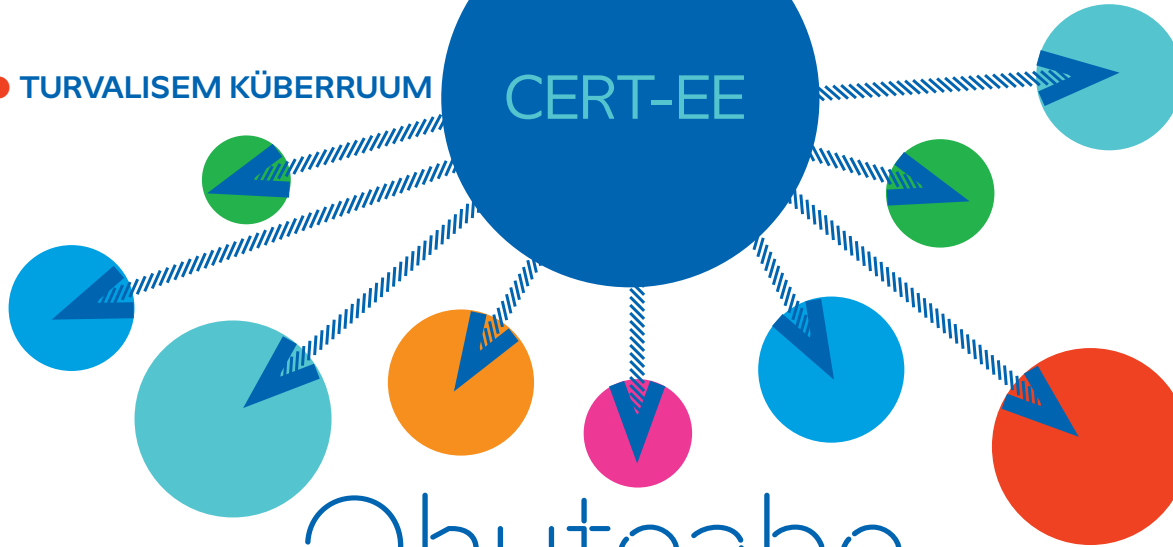
Kordasime erinevates kanalites regulaarselt üle teada-tuntud kübertõdesid ning lisasime neile kaugtöö ja -õppe kohta käivad põhisõnumid.

### Fookus kaugtöö turvalisusel

Märtsis ootamatult kodutööle ja -õppele jäänud inimestel oli vaja mitmel suhtlusplatvormil kiirkorras luua uus konto. Samuti kasvas elektrooniline infovahetus töökoha, kooli ja e-teenuste pakkujatega, mis kõik kokku lõi soodsa pinnase küberintsidentidele.

Kordasime erinevates kanalites regulaarselt üle teada-tuntud kübertõdesid (uuenda tarkvara, ära kliki kahtlastele linkidele, ära sisesta oma PIN-koodi suvalisse kohta, varunda andmeid) ning lisasime neile kaugtöö ja -õppe kohta käivad põhisõnumid.

Lisaks saime vähem kui kolme nädalaga paberilt avalikkuse ette kogu kaugtöö tegijatele suunatud teavituskampaania, mis selgitas, kuidas tagada küberturvalisus ka kodukontoris (vt ka lk 30).




# Ohuteabe väljasaatmine nüüdsest automaatne

**CERT-EE** saadab iga päev Eesti telekomifirmadele, veebiteenuste majutajatele ja oma võrke haldavatele asutustele automatiseeritud teateid kuritarvituste ja haavatavuste kohta nende võrkudes. Pahatihti ei jõua see info sealt edasi lõppkliendini.

2020. aasta esimeses kvartalis teatas üks Eesti energiasektori ettevõte CERT-EE-le intsidendist oma serveris. Nad andsid märku, et internetis oli avalikult kättesaadavaks jäänud teenus nimega memcached, mille ülesanne on hoida oma teenuse tarbeks infot ajutiselt puhvris. Kuid seda on võimalik ka kurjasti ära kasutada teenustõkestusrünnakutes internetiliikluse võimendamiseks: saadad ühe paketi teenusele sisendiks, saad kuni 500 000-kordselt infot vastu. Ning puhvrisse jäänud info lekib. Sellisest rünnakust ja lekkest CERT-EEd teavitatigi.

Intsident polnud kuigi erakordne. Ettevõte sai oma teenuse korda, CERT-EE aitas logid üle vaadata ja andis oma soovitused. Oluliseks teeb selle asjaolu, et tegelikult oli CERT-EE ettevõttele internetiteenuse pakkujat avatud memcached teenusest korduvalt teavitanud, kuid sealt ei liikunud ohuteavitus energiasektori ettevõtteni edasi. Sarnaseid näiteid, kus ohuteadete edastamine oleks intsidendist päästnud, võib tuua mitu.

## Saadame ohuteavitusi iga päev

Alates 2019. aasta suvest on CERT-EE saatnud vähemalt kord ööpäevas Eesti telekommunikatsiooniettevõtetele, veebiteenuste majutajatele ja oma võrke haldavatele asutustele

automatiseeritud teateid kuritarvituste ja haavatavate seadmete/seadistuse kohta nende võrkudes.

CERT-EE saab vastava info omakorda partneritelt, kes skaneerivad tervet internetti või koguvad oma töö käigus kokku hulga indikaatoreid, mis näitavad, kus on turvanõrkused, tuntud nakatumised, kust algavad jõurünnakud ja kust skaneeritakse teisi.

Meie automatiseeritud süsteem korjab teavitused kokku, sorteerib ning saadab need omakorda edasi kas Eestisse registreeritud võrkude teenusepakkujale või siis suuremate-le asutustele, kelle IP-vahemikud meile teada on. Nemad peaksid info edasi saatma lõppkasutajatele, sest lõpuks vastutab süsteemide turvalisuse eest nende omanik.

### Üle 800 000 nakatumisteate

Automaatteavituste tõttu võib paista, et intsidentide hulk, millega CERT-EE tegeleb, on viimastel aastatel vähenenud – 3164 pealt 2019. aastal 2762-le 2020. aastal –, kuid see arv näitab ainult neid intsidente, millele CERT-EE tehnikud on käed külge pannud.

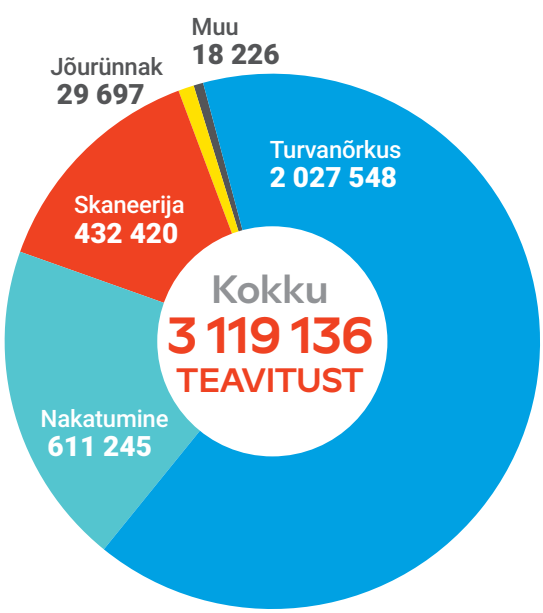
Näiteks lõpetasime 2020. aasta juulist robotvõrgustike Avalanche ja Necurs nakatumiste kajastamise CERT-EE intsidentide loetelus ja suunasime need teated samasse automatiseeritud süsteemi, et vähendada spetsialistide käsitööd. Avalanche'i robotvõrgustik peatati rahvusvahelise politseioperatsiooni tulemusel juba 2016. aasta detsembris, kuid nakatumised jätkusid hiljemgi, ja Necursi võrgustiku sai Microsoft enda kontrolli alla 2020. aasta märtsis, mistõttu võib hinnata, et need kaks võrgustikku enam aktiivselt küberruumi ei ohusta. Ilma metoodikat muutmata olnuks 2020. aasta intsidentide hulk 3439 ehk suurem kui varasematel aastatel.

2020. aastal andsime niimoodi Eesti teenusepakkujatele märku enam kui 800 000 nakatumisest enam kui 2000 IP-aadressilt. Selle hulgas on palju korduvaid nakatumisi, aga ka pahavarasid, mis tegelikult on juba neutraliseeritud, kuid mis jäävad arvutitesse edasi „tiksuma" kauaks pärast nende puhastamist.

Mida rohkem seadmeid on internetti ühendatud ja mida paremini oskavad küberturvalisuse spetsialistid oma tööd teha, seda enam avastatakse turvanõrkusi, nakatumisi ja pahaloomulist internetiliiklust. Ohuteabe automatiseeritud jagamine võrkude omanikele on seega ainuvõimalik samm küberturvalisuse taset hoida. Kuid nagu alguses kirjeldatud intsident näitab, ei piisa sellest, kui CERT-EE info välja saadab, teenusepakkujad peavad selle edastama ka lõppkliendile.

> 2020. aastal andsime Eesti teenusepakkujatele märku enam kui 800 000 nakatumisest enam kui 2000 IP-aadressilt.

## Automatiseeritud teavitused juuli–dets 2020



# RIA kaitseb Eesti demokraatiat

Selleks, et 2021. aasta sügisel toimuvad kohalike omavalitsuste valimised sujuksid tõrgeteta ja turvaliselt, on RIA saanud endale ülesandeid juurde. Vaatame valimiste küberturvalisust ja seega demokraatia toimimise kaitsmist väga laia pilguga.

E-valimiste puhul saab enamasti kõige rohkem tähelepanu e-hääletamise süsteem, mille nähtavaim osa on valijarakendus. Kuid kõige rangemaid meetmeid on aga vaja häälte kokku kogumiseks kasutatava rakenduse ehk Koguja turvamiseks. Sinna saadavad valijad oma arvutitest e-hääled krüpteerituna. Kogujat majutab RIA.

Samas on meil vaja hoolitseda ka selle eest, et valijarakendus jõuaks valijani õigest kohast (et keegi ei meelitaks valijaid oma seadmesse pahavara tõmbama) ja et uuendamata tarkvara ei takistaks valijal hääletada.

## Kandidaadid ja parteid

Teiste riikide kogemusest teame, et ründajad võtavad tihtipeale sihikule mitte valimiste korraldajad, vaid kandidaadid või erakonnad. Nii on juhtunud USAs, Prantsusmaal ja mujal. Kandidaatide ja erakondade koduleheküljed, nende sotsiaalmeedialehed või ka meiliserverid võivad sattuda kas riikliku taustaga ründaja sihtmärgiks või trollide saagiks.

RIA küberturvalisuse teenistus korraldab ka tänavu kandidaatidele ja kampaaniameeskondadele küberhügieenikoolitused, kus annab nõu, kuidas oma kontosid turvata ning kuidas tunda ära rünnakuid. Küberhügieenikoolituste kõrval pakub RIA erakondadele võimalust saada tasuta ülevaade oma veebi- ja meiliserverite turvaprotokollidest ning nõuandeid turvapildi parandamiseks.

### Uus valimiste infosüsteem

Samas on valimiste toimimiseks vaja palju muidki arendusi ja tehnoloogiaid. Valijate ja kandidaatide nimekirjade haldamiseks, paberhäälte lugemiseks valimisjaoskondades ning e-hääletuse tulemuse talletamiseks vajaliku valimiste infosüsteemi (VIS) teine versioon on kasutusel olnud juba pikalt ning selle komponendid ei vasta enam tänapäeva infoturbe parimatele praktikatele. Seetõttu alustas RIA valimisteenistuse tellimusel VISi kolmanda versiooni arendamist. VIS3 saab valmis 2021. suveks, turvatestimise järel saab selle sügisel kasutusele võtta.

VIS3 on oluline arendus ka valimisseaduse muudatuse tõttu, mis nõuab, et sellest aastast võetaks kasutusele elektroonilised valijate nimekirjad (seni trükiti need paberile välja) ning oleks võimalik e-hääletada ja paberil

hääletada samal ajal. See tähendab näiteks ka seda, et hääletada saab ükskõik millises valimisjaoskonnas üle Eesti ning samuti on sel sügisel võimalik oma e-häält jaoskonnas muuta veel valimispäevalgi.

Kõige selle jaoks on oluline, et VIS3 töötaks õigel ajal, et õigetel inimestel oleks korrektsed ligipääsud, et kõik teised andmebaasid (rahvastikuregister, äriregister, vanglaregister jt) oleksid kättesaadavad ja keegi ei saaks näiteks kandidaatide piirkonda valeks muuta.

### Kõik peab toimima nagu kellavärk

VIS3 on ka see platvorm, kus valimiste tulemused kokku loetakse ja kust valimiste kodulehekülg õigel ajal õiged andmed saab. See tähendab, et koduleheküljelegi tuleb valimiste õhtul pöörata palju rohkem tähelepanu kui muidu: kui kompromiteerida koduleht ja muuta valimistulemust ainuüksi kodulehel, on sellel suur mõju valimiste usaldusväärsusele.

Kõigi nende tehnoloogiate kõrval pöörame tähelepanu ka teistele süsteemidele, millest Eesti valimised sõltuvad: elektrooniline identiteet, erinevad registrid, riigivõrk, kohalike omavalitsuste internetiteenus. Kui mõnel päeval on lühiajaline katkestus mõnes neist aktsepteeritav, siis valimiste perioodil peab kõik toimima nagu kellavärk.

## Kes mida teeb?

2021. aasta jaanuaris sõlmisid **majandus- ja kommunikatsiooniministeerium** (MKM), **riigi infosüsteemi amet** (RIA) ja riigi **valimisteenistus** (RVT) koostöölepingu, et määrata kindlaks asutuste ülesanded elektroonilise hääletamise korraldamisel ja valimiste küberturvalisuse tagamisel.

**RVT** ülesanne on e-hääletuse süsteemi (EHS) arendamine ja haldamine, süsteemi turvatestimise korraldamine ja riskianalüüsi läbiviimine ning valimiste e-hääletamisega seotud andmete töötlemine. Valijate ja e-hääletuse korraldusega seotud osapoolte küsimustele vastamist ning valimiste veebilehe arendamist ja selle sisu haldamist korraldab samuti RVT.

**RIA** toetab RVTd tehnilistes küsimustes ning kõige tähtsam ülesanne on korraldada VIS3 ja sellega seotud veebide tehnilist arendamist. RIA osutab nende süsteemide majutus- ja haldamisteenust. Ameti ülesandeks saab ka valimiste küberturvalisusalaste teavitustegevuste korraldamine.

**MKM** viib tänavu 1. oktoobriks läbi valimiste infosüsteemi (VIS3) ja EHSi küberturvalisuse auditi ja analüüsi ning annab vabariigi valimiskomisjonile enne valimisi hinnangu, kas valimiste küberturvalisuse nõuded on nii VIS3 kui EHSi osas täidetud ning turvameetmed asjakohased ja korrektselt rakendatud.

# Valmis Eesti uus infoturbe-standard

RIA eestvedamisel valmis mitut aastat töös olnud **Eesti infoturbestandard** (E-ITS), mis vahetab 2024. aastaks välja seni kasutusel olnud ISKE.

Riigil ja kohalikel omavalitsustel on palju andmeid ja andmekogusid. Näiteks inimeste terviseandmeid sisaldav tervise infosüsteem (TIS) või Rakvere linna toetuste taotlemise ja menetlemise süsteem. Andmekogud aitavad efektiivsemalt asju ajada, asutustevahelist infovahetust korraldada, langetada otsuseid ja riigil riigina toimida.

Suur osa neist andmetest on tundlikud ja neid tohivad kasutada vaid need, kellel selleks õigus. Teiste ees on uks suletud. Seda, millistele nõudmistele peaks uks vastama ja kuidas kontrollitakse, kes saab sellest sisse astuda, aitabki tagada ISKE ehk infosüsteemide turvameetmete süsteem.

Toome uuesti näiteks terviseandmed, mille puhul peab olema tagatud nende konfidentsiaalsus (neid ei saa igaüks sirvida), terviklikkus (neid ei saa omavoliliselt muuta ega kustutada) ning käideldavus (arst peab saama neid vajalikul hetkel kasutada).

Varemalt ISKE ja nüüd E-ITS on eeskätt avalikule sektorile loodud tööriist, millega tagada, et kõigi avalikke ülesandeid täitvate asutuste infoturve oleks võrreldaval tasemel.

## Selgem ja lühem

2004. aastast kehtiv ja oma umbes 5000 lehekülje hoomamatult mahukas ISKE pole just kõige parema mainega. Selle uuendamine peatus 2018. aastal, kui lõpetati selle alus-


standardiks olnud Saksa versiooni uuendused. Seetõttu oli vaja kiiret asendust.

ISKE kõrvale loodi võimalus rakendada rahvusvaheliselt tunnustatud standardit ISO/IEC 27001. Paraku on selle rakendamine jõukohane infoturbe- ja riskihaldusteadlikele ja -võimekatele organisatsioonidele.

E-ITSi eesmärk on esitada organisatsioonidele infoturbe käsitlemiseks eestikeelne ja Eesti õigusruumile sobiv alus, mis oleks vastavuses ISO/IEC 27001 standardiga. E-ITS pakub infoturbe etalonmeetmed ja rakendamise süsteemi, mis aitab organisatsioonil saavutada selle vajadustega sobiva infoturbe taseme.

Mida paremini suudame E-ITSi rakendada, seda kindlamini suudame toime tulla ootamatustega, olla oma tegevustes läbipaistvamad ning tagada usaldus riigi infosüsteemide ja riigi vastu tervikuna.

**Eeskätt avaliku sektori tööriist**

Avaliku sektori töötajatele peaks E-ITSi kasutamine saama tööprotsessi loomulikuks osaks, mis on vajalik konkreetsete riskide realiseerumise vältimiseks.

E-ITS on nagu kortermaja, kuid iga korteri sisustab selle omanik vastavalt enda vajadustele ja soovidele.

Kaheastmeline infoturbestandard E-ITS on nagu kortermaja, mis on valminud vastavalt seadustele ja nõuetele. Kuid iga korteri sisustab ja kujundab selle omanik vastavalt enda vajadustele ja soovidele. Seal, kus riskinormid on kõrgemad, tuleb lisada oma meetmeid.

Loodame, et uus infoturbestandard võetakse lähiaastatel omaks ja et iga organisatsioon avastab kasulikud nipid, kuidas infoturbe riskidega paremini ja lihtsamalt toime tulla.

Eesti infoturbestandard koostati Euroopa Liidu struktuuritoetuse toetusskeemi „Infoühiskonna teadlikkuse tõstmine“ raames Euroopa Regionaalarengu Fondi rahastusel.

E-ITSiga seonduvad materjalid on koondatud veebilehele eits.ria.ee.

2023 | 2024

**MÄRTS**
- Algab pilootrakendamine
- Portaal avaldab uue standardi

**APRILL**
- Koolitused standardi rakendajatele

**DETSEMBER**
- Esimesed asutused on uue standardi järgi auditeeritud

**DETSEMBER**
- Senised ISKE rakendajad on uuele standardile üle läinud

**JAANUAR**
- Jätame ISKEga lõplikult hüvasti

# DigiTest aitab parandada küberhügieeni

Alates 2017. aastast pakub RIA koostöös küberturbeettevõttega CybExer Technologies avaliku sektori asutuste töötajatele küberhügieeni õppeplatvormi **DigiTest**, mille on praeguseks läbinud üle 15 000 kasutaja.

On reede õhtu. Pikk ja väsitav töönädal on äsja lõppenud. Raamatupidaja hakkab arvutit sulgema, kui märkab, et tema postkasti saabub kiri ülemuselt. „Tere, Anne! Manuses on arve, mille unustasin varem edastada. Maksetähtaeg oli juba üleeile. Palun kanna see 40 000 neile kohe üle! Muidu hakkab viivis tiksuma. Aitäh! Kaja“. Mida teeksid raamatupidaja asemel samasuguses olukorras?

Kuidas tunda ära arvepettuseid ja õngitsuskirju? Kuidas luua turvalisi salasõnu? Kuidas kasutada avalikke WiFi-võrke ja väliseid andmekandjaid nii, et sinu ega tööandja andmetele ei pääseks ligi kõrvalised isikud?

Neid ja paljusid teisi küberhügieeni teemasid katab DigiTest, mille on läbinud üle 15 000 avaliku sektori töötaja.

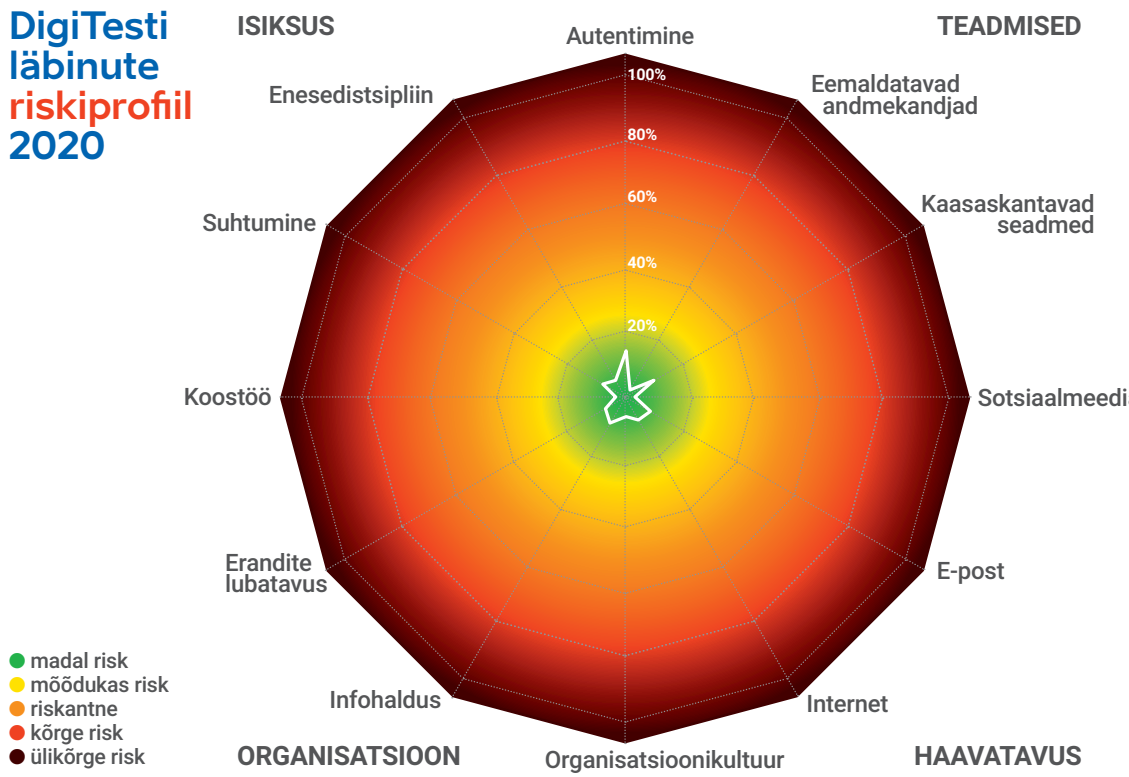
### Küberturvalisus algab arvutikasutajast

Küberturvalisuse õppeplatvorm DigiTest valmis 2017. aastal ja selle eesmärk on tõsta küberturvalisusalast teadlikkust, kuna see on kõige tõhusam viis hoida ära väiksemaid ja suuremaid küberintsidente.

Kursuse läbimise järel koostab süsteem antud vastuste põhjal kasutaja riskiprofiili ja toob välja kõrgema riskiga valdkonnad, millele võiks rohkem tähelepanu pöörata. Sama-

## DigiTesti läbinute suuremad riskid aastatel 2018–2020

| 2018 | 2019 | 2020 |
|---|---|---|
| **E-post** (25%): näitab, kas arvutikasutaja mõistab e-postiga kaasnevaid ohtusid. Näiteks kas tunneb ära õngitsuskirja. | **Infohaldus** (16%): näitab, kas arvutikasutaja mõistab ja järgib organisatsioonile olulisi turvareegleid. | **Autentimine** (14%) |
| **Internet** (24%): näitab, kas arvutikasutaja tajub internetiga kaasnevaid ohtusid. Näiteks kas ja kuidas kasutab avalikke WiFi-võrke. | **Internet** (14%) | **Kaasaskantavad seadmed** (10%) |
| **Autentimine** (24%): näitab, kuidas kasutaja loob ja hoiab salasõnu, kas kasutab mitmeastmelist autentimist jmt. | **Kaasaskantavad seadmed** (9%): näiteks kuidas kaitsta mälupulgale salvestatud andmeid. | **E-post** (9%) |




moodi annab DigiTest vastava asutuse infoturbe eest vastutavale isikule organisatsiooni koondpildi. Selle põhjal saab selgeks, millistes küberhügieeni valdkondades oleks vaja kolleege koolitada, et riskantset käitumist ja sellega kaasnevaid ohte vähendada.

### Tase on aasta-aastalt parenenud

Pannes kokku DigiTesti tuhandete kasutajate koondpildi ning võrreldes selle muutust aastate lõikes, võime öelda, et tulemus on hea ja aasta-aastalt parenev.

DigiTest mõõdab erinevate valdkondade riske 100 protsendi skaalal, kus null tähistab riski puudumist ja 100 maksimaalset riski. Kui 2018. aastal olid kolm kõige riskantsemat valdkonda vahemikus 24–25 protsenti, siis eelmisel aastal 9–14 protsenti.

Kolme aasta eest seostusid enim muret valmistanud valdkonnad e-postiga (nt kas kasutaja tunneb ära õngitsuskirju), internetiga (nt kas ja kuidas kasutada avalikke WiFi-võrke) ja autentimisega (nt kuidas luua ja hoida salasõnu ning kasutada mitmeastmelist autentimist).

Mulluses riskide esikolmikus jätkasid e-post ja autentimine, kuid internet asendus kaasaskantavate seadmetega (nt kuidas avalikus kohas turvaliselt sülerit kasutada või kaitsta mälupulgal olevaid andmeid).

RIA eesmärk on, et kõik avaliku sektori töötajad läbiksid DigiTesti või mõne muu küberõppeplatvormi vähemalt kord aastas. Nii aitame kinnistada olemasolevaid teadmisi teada-tuntud ohtude kohta, aga anda ka uut infot värskete riskide kohta.

> Eesmärk on, et kõik avaliku sektori töötajad läbiksid kord aastas mõne küberhügieeni testi.

# Teavitus-kampaaniad küberturvalisuse teenistuses

RIA korraldab regulaarselt ennetus- ja teavituskampaaniaid, et parandada Eestis küberturvalisuse taset. Eelmisel aastal olid fookuses kaugtöö tegijad, väikesed ja keskmise suurusega ettevõtted ning vene emakeelega eakad.

2019. aasta sügisel toimus vanemaealistele suunatud teavituskampaania „Ole IT-vaatlik!“. Selle edust tiivustatuna planeerisime 2020. aastasse kaks mahukamat kampaaniat: esimene suunatud väikestele ja keskmise suurusega ettevõtetele ning teine taas vanemaealistele eestimaalastele, seekord fookusega vene emakeelega inimestele.

Vahel teeb elu plaanidesse korrektiive: kahe mainitud kampaania ulatusele pani põntsu COVID-19 teine laine. Samas lisandus koroonaviiruse tõttu kevadise eriolukorra ajal veel kolmas, mis keskendus turvalisele kaugtööle. See jõudis koostöös eelmisegi korra kampaaniapartneriga Havas aprillis ideefaasist avalikkuse ette vähem kui kolme nädalaga.

## Ole eriolukorras eriti IT-vaatlik!

2019. aasta sügisel hüüdlausena kõlanud „Ole IT-vaatlik!“ jäi paljudele positiivselt meelde, mistõttu otsustasime ka pool aastat hiljem kasutada sama lahendust ning tuttavat värviskeemi. Läbiv sõnum oli sel korral „Ole eriolukorras eriti IT-vaatlik!“.

Kampaania väljundiks olid aprilli lõpus ja mai alguses kahe nädala vältel kohalike meediaportaalide reklaambänneritel ning tele- ja raadioreklaamides levitatud küberturvalisuse põhitõed. Neid vürtsitasime tõsiasjaga, et seoses hüppeliselt kasvanud kaugtöö tegemisega on rohkem ka võimalikke komistuskohti.

## Kaitse ettevõtet küberrünnaku eest

Septembris ja oktoobris pöörasime pilgud väikeste ja keskmise suurusega ettevõtete suunas. Jätkasime juba sissetöötatud hüüdlausega „Ole IT-vaatlik“, millele lisasime „Kaitse ettevõtet küberrünnaku eest!“. Kampaaniapartneriteks olid reklaamiagentuur Age, sõnumiagentuur Akkadian ja konsultatsiooniettevõte Haap Consulting. Kampaaniaperioodil jooksid teles ja raadios reklaamklipid, kaunistatud said Tallinna bussiootepaviljonid ja valgusvitriinid, ajalehtedes ilmusid arvamuslood, sotsiaalmeedias vilkusid bännerid.



Kuigi naasev COVID-19 hakkas taas kimbutama, leidsid suuremates linnades aset mitmed üritused, kuhu kampaania sõnumid tänu RIA ja erasektori esindajatele kas ettekandena või vestlusringide vahendusel kohale jõudsid.

### Eriline tähelepanu muukeelsetele eakatele

2019. aasta vanemaealistele suunatud kampaania järeluuring näitas, et kõige vähem jõudsime sellega eakateni, kelle emakeel pole eesti keel. Seetõttu korraldasime Havasiga eelmise aasta viimastel kuudel jätkukampaania, mille sihtgrupiks just nemad.

Paraku takistas koroonaviiruse teine laine seda juba üsna tõsiselt. Kuna vanemaealised on viiruse riskigrupp, ei saanud me läbi viia plaanitud koolitusi ega muid kontaktseid üritusi ei Ida-Virumaa ega Tallinna raamatukogudes.

Selle asemel salvestasime pikemad koolitusvideod ning peamisi küberohte tutvustavad videod. Korraldasime ka virtuaalsed küberkoolitused raamatukogude töötajatele, kes edaspidi oma kliente arvuti ja nutiseadmetega seotud küsimustes veel paremini aidata oskavad. Avaldasime pressiteateid, esinesime ETV+ ja Raadio 4 eetris ning koostöös Teliaga töötas Tallinna keskraamatukogus novembris ja detsembris igal kolmapäeval infoliin, millele helistades sai asjakohast abi.

### Mis edasi?

Järgmise suurema teavituskampaania suuname enne 2021. aasta oktoobris aset leidvaid kohalikke valimisi IT-teadlikule e-hääletajale. Veel enne seda, septembri alguses, tahame avalikkuse ette tuua uue ja täiustatud versiooni leheküljest itvaatlik.ee, kuhu seni on maandunud lõppenud kampaaniad, kuid mis peaks aja jooksul kujunema arvestavataks küberturvalisusalaseks ennetus- ja teavitusveebiks.

Järgmistel aastatel soovime teha vajaduspõhiseid ja sihistatud kampaaniaid nendele gruppidele, kelle poole suunavad statistika ja uuringud. Loomulikult oleme valmis paindlikult reageerima, nagu kevadise eriolukorra ajal. Kõige selle saavutamiseks vajame püsivat eelarverida, mis võimaldaks oma tegevusi pikemalt ja paremini ette planeerida.

# Kuidas tagada 5G-võrkude turvalisus?

Sellest, kuidas leida tasakaalupunkt riigi julgeoleku ja sideettevõtjate huvide vahel, kirjutab riigi küberturvalisuse poliitika juht **Raul Rikk.**

Uue generatsiooni sidevõrkude turvalisus on viimastel aastatel olnud üks olulisemaid küberturbe teemasid. Seda nii riiklikult kui rahvusvaheliselt, nii Euroopa Liidus kui maailmas laiemalt. Pole ka ime, sest arenenud ühiskondade toimimine sõltub peaaegu täielikult side- ja infosüsteemidest. 5G- ja uuema põlvkonna võrgud süvendavad seda sõltuvust veelgi, kuna sideühenduste arv ja kiirus kasvab praegusega võrreldes mitu korda.

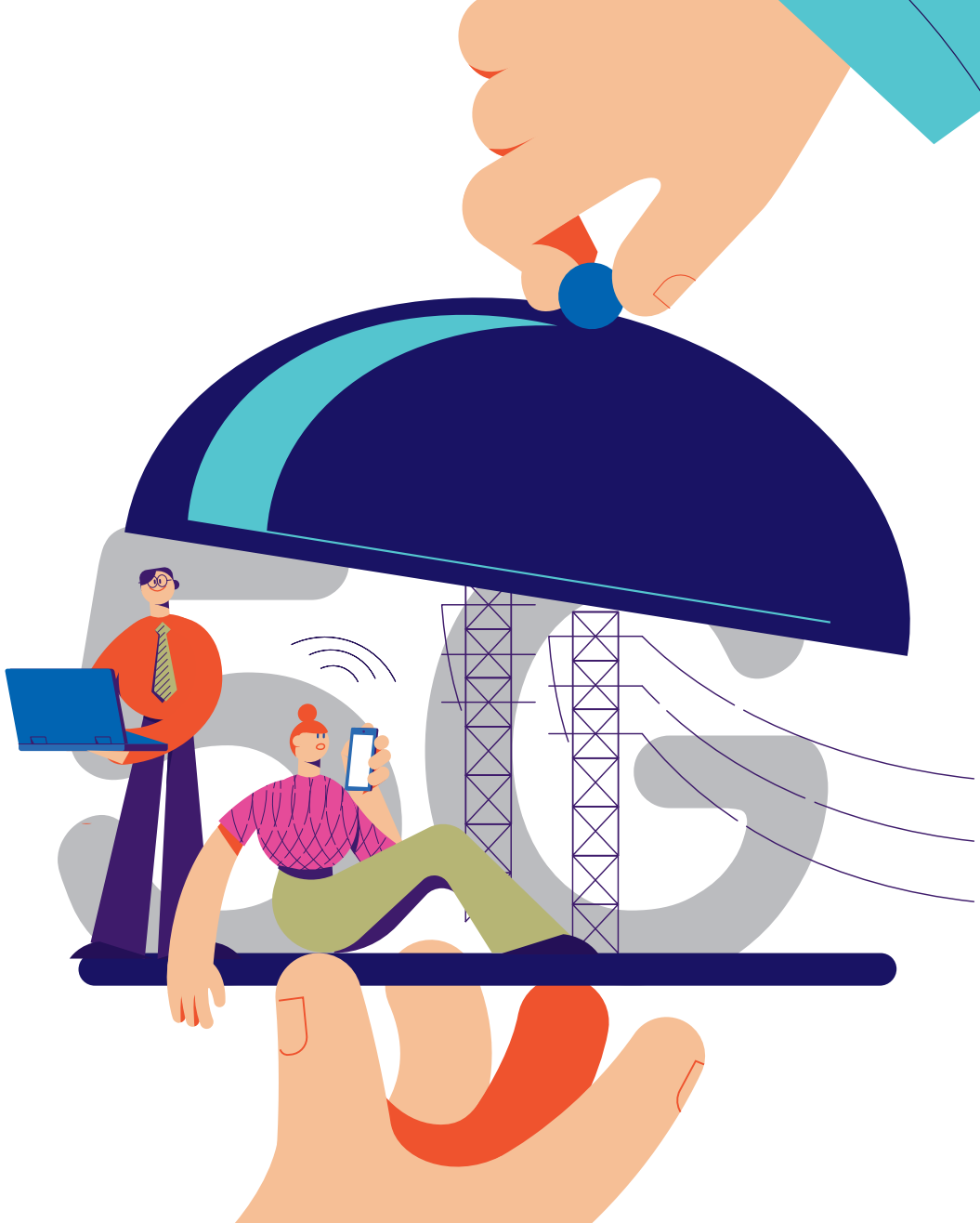
## Turvalisusest ei saa üle ega ümber

Arvata võib, et lähitulevikus on peaaegu kõik seadmed ühendatud sidevõrkudesse ja internetti – nutividinad, isesõitvad autod, robotid, meditsiiniseadmed ja paljud muud elutähtsad seadmed.

See on küll tohutult mugav, kuid teisalt seab turvalisusele väga kõrged ootused. Kuna kõik andmed liiguvad läbi sidevõrkude, muudab see sidetaristu digitaalsete infoühiskondade jaoks strateegilise tähtsusega infrastruktuuriks.

Samal ajal pole meil võimalust tehnoloogiate turvalisust tehniliselt kontrollida, sest see on väga kompleksne ning disainitud, toodetud ja kokku pandud väljaspool Eestit. Nüüdisaegsed seadmed on niivõrd keerulised, et praktikas on võimatu hinnata, kas need sisaldavad pahavara, tagauksi või olulisi turvanõrkusi. Keerukust lisavad sagedased tarkvarauuendused ja kriitilised turvapaigad, mille paigaldamisega pole aega oodata.

See pole probleem ainult Eesti, vaid kõikide jaoks. Isegi suurtel riikidel nagu USA, Ühendkuningriik, Prantsusmaa või Saksamaa on pii-



# Ajajoon 5G 2019

## ARENGUD EUROOPA LIIDUS

**12. märts**

- Euroopa Parlamendi aruanne

**22. märts**

- Euroopa Ülemkogu järeldused

**26. märts**

- Komisjon avaldas soovituse, et liikmesriigid võtaksid kasutusele konkreetsed meetmed 5G-võrkude küberturvalisuse riskide hindamiseks ja riskimaandamismeetmete tugevdamiseks

ratud võimekus riist- ja tarkvara kontrollida, hoolimata sellest, et neil on suured, umbes tuhande või enama inimesega küberturbeasutused.

### Koostöö alus on usaldus

Seega, oleme jõudnud olukorda, kus digiriigi turvalisus põhineb tehnoloogia tootja usaldamisel. Tehnoloogia tootja pole enam pelgalt seadmete ja tarkvara tarnija, vaid laiemalt tehnoloogilise teenuse pakkuja, kellega ehitatakse üles aastatepikkune koostöösuhe.

Küsimus pole ühes ettevõttes või selle tehnoloogias, vaid laiem – kas saame lahenduste pakkujaid usaldada oludes, kus tehnoloogia sisuline kontroll on lõpuni võimatu. Usalduse hindamisel peame arvestama olusid, milles tehnoloogiat toodetakse – näiteks tootja asukohariigi seadusruumi ja julgeolekualast käitumist.

Euroopa Liidu liikmesriigid avalikustasid 2020. aasta alguses ühise meetmete paketi, mis loob aluse 5G-sidevõrkude julgeoleku tagamiseks. Selles öeldakse, et liikmesriigid peaksid karmistama mobiilside operaatorite turvanõudeid, hindama tehnoloogia tarnijate riskiprofiili ning kohaldama piiranguid kõrge riskiga tarnijate suhtes. Samuti on vaja tagada, et sideteenuse osutajad kasutaksid asjakohaselt mitme tehnoloogiatootja riist- ja tarkvara, et vältida suurt sõltuvust ühest tarnijast ning kõrge riskiga tehnoloogia tootjast.

### Sidevõrkude turvalisuse määrus

Euroopa Liidu liikmesriikide vahel kokku lepitud meetmete rakendamiseks on majandus- ja kommunikatsiooniministeerium tihedas koostöös erinevate riigiasutuste ja sidevõrgu ettevõtjatega töötanud viimase kahe aasta jooksul sidevõrkude turvalisuse määruse kallal. Regulatsiooniga tahetakse tagada, et sidevõrkude rajamine ja nende vahendusel sideteenuste osutamine toimuks turvalise tehnoloogia abil ning et seda teeks usaldusväärne partner. Selleks on vaja ühest küljest välistada kõrge riskiga tehnoloogia ning teisest küljest rakendada lubatud tehnoloogiale asjakohaseid turvameetmeid.

Seda, kas ja mis on kõrge riskiga tehnoloogia ning millist ohtu see kujutab meie riigi julgeolekule, hinnatakse riist- ja tarkvara kasutusloa menetluses. Sideettevõtjal tuleb enne tehnoloogia kasutusse võtmist esitada kasutusloa taotlus. Seda menetleb valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu, mis hindab, kas tegemist on kõrge riskiga riist- või tarkvaraga või kas selle kasutamine võib ohustada riigi julgeolekut muul põhjusel.

> Oleme jõudnud olukorda, kus digiriigi turvalisus põhineb tehnoloogia tootja usaldamisel.

Eelnõu järgi rakendub kasutusloa kohustus ning kõrge riskiga riist- ja tarkvara keeld riist- ja tarkvarale, mis plaanitakse kasutusele võtta pärast määruse jõustumist. Lisaks rakenduvad mõlemad ka juba olemasolevale tehno-

**2019**

**9. oktoober**
Liikmesriigid viisid lõpule 5G-võrkude turvalisust käsitleva, ELi koordineeritud riskihindamise uue standardi

**21. november**
Euroopa Liidu küberturvalisuse amet (ENISA) avaldas aruande 5G-võrkudega seotud ohtude kohta

**2020**

**29. jaanuar**
Liikmesriikide võetavate leevendusmeetmete paketi avaldamine. Komisjoni teatis ELi meetmepaketi rakendamise kohta

loogiale, milles on võetud või võetakse kasutusele 5G või uuemad funktsioonid.

Kasutusloa kohustus ja kõrge riskiga tehnoloogia keeld on planeeritud etappide kaupa. tuumikvõrkude puhul hakkavad need kehtima kohe pärast määruse jõustumist, kuid 5G- ja uuemate võrkude puhul antakse üleminekuaeg. See tähendab, et 5G- võrkude puhul tuleb kasutusluba hakata taotlema kohe, kuid kõrge riskiga riist- ja tarkvara on lubatud kasutada kuni 31. detsembrini 2025. Muus sidevõrgu osas antakse üleminekuajaks üheksa aastat ehk kuni 2030. aasta alguseni.

### Otsides tasakaalupunkti

Kuigi eesmärk on selge – sideteenuse osutamisel kasutatav riist- ja tarkvara ei tohi ohustada riigi julgeolekut –, on olnud palju arutelu ja eriarvamusi, kuidas selleni jõuda.

Arusaadavalt võib selline regulatsioon sideettevõtjatele kaasa tuua kulutusi. Oleme siin püüdnud leida tasakaalupunkti riigi julgeoleku tagamise ja sideettevõtjate huvide vahel. Seetõttu on otsustatud üleminekuaja kasuks. See annab ettevõtetele võimaluse oma äritegevus üle vaadata ja teha vajalikke muudatusi, kuid teisalt tagab tulevikus 5G- ja muu IKT-taristu turvalisuse.

2020. aasta sügisel toimus eelnõu avalik konsultatsioon, pärast seda tegime eeskätt ettevõtjate tagasiside pinnalt ja nende huvisid arvestades eelnõus muudatusi: näiteks pikendasime 5G-võrkude osas üleminekutähtaega varasema kolme asemel viie aastani.

2021. aasta märtsis soovis õiguskantsler, et enne määruse vastuvõtmist täiendataks elektroonilise side seadust. Loodame määrusega võimalikult kiiresti edasi liikuda, sest turbemäärus on võtmetähtsusega ka meie 5G sageduskonkursside jaoks – sageduste jagamisega saame alustada siis, kui turvalisuse nõuded on paigas.

Eelnõu osas kokkuleppele jõudmine on kõigi huvides, sest kokkuvõttes kaotavad kõige enam sideettevõtjad ja nende kliendid, kui uue põlvkonna sidelahendustega ei saa edasi liikuda. Eesti jaoks on aga oluline, et need uued sidelahendused ja IT-taristu laiemalt oleksid usaldusväärsed ja vabad kõrge riskiga tehnoloogiast. See on oluline nii julgeoleku tagamiseks kui ka meie digiriigi suhtes usalduse hoidmiseks.

## ELi meetmepakett 5G-võrkude turvalisuse tagamiseks

Liikmesriigid peaksid rakendama meetmeid ja neil peaks olema volitus riskide leevendamiseks. Eelkõige peaksid nad käsitlema järgmisi aspekte:

- mobiilsideoperaatorite turvanõuete karmistamine,
- tarnijate riskiprofiili hindamine; asjakohaste piirangute kohaldamine suure riskiga tarnijate suhtes, sealhulgas vajalikud erandid põhivarade puhul,
- tagamine, et igal operaatoril on asjakohane mitme teenuseosutajaga strateegia, et vältida või piirata suurt sõltuvust ühest tarnijast ning hoida ära sõltuvust suure riskiga tarnijatest.

**30. aprill**

- Komisjon kutsub liikmesriike üles astuma esimesi konkreetseid ja mõõdetavaid samme põhimeetmete rakendamiseks

**30. juuni**

- Komisjon kutsub liikmesriike üles koostama aruande liikmesriikide võetud põhimeetmete rakendamise kohta

**Oktoobriks**

- Komisjon kutsub liikmesriike üles koostama aruande liikmesriikide võetud põhimeetmete rakendamise kohta

# Küberturvalisus pole Javelini rakett, mida saab lasta ja unustada

Digitaalne maailm jõuab meie igapäevaellu üsna iseseisvalt, kuid turvalisusega peab iga inimene ja organisatsioon ise aktiivselt tegelema, kirjutab keskkriminaalpolitsei küberkuritegude büroo juht **Oskar Gross**.

Küberkuritegevus on olnud aastaid kasvutrendis ning arvestades hoogsat digiteerumist, võib eeldada, et see tempo ei aeglustu. Tihti räägitakse, mis on küberkuritegevuses uut või teistmoodi, kuid tuleb rõhutada, et küberturvalisuse põhimõtted ei ole ajas oluliselt muutunud. Üsna ilmekalt demonstreerib seda ligi 14 aasta tagune Kalmer Viska artikkel „Küberkuritegevus – kas seda saab ära hoida?“, mis laias laastus käsitleb täpselt samu teemasid, millest räägime tänapäeval. Ka artiklis välja pakutud lahendused – küberhügieen ja kriitiline mõtlemine – pole sugugi aegunud, kuid peame neid oluliselt rohkem rakendama.

## Näha pole, aga maksab palju

Ei ole mõtet tolmu vaiba alla pühkida – kvaliteetne küberturvalisus on kulukas, eriti võrreldes lihtsama „ühenda ja mängi“ lahendusega. Hea paralleeli võib tuua autoga korralises hoolduses käimisega: töökojast välja sõites oled ilma mitmesajast eurost, aga aru ei saa, et sõiduki juures oleks midagi muutunud. Samas teame ju kõik, et kui jätta õli ja filtrid vahetamata, võib puksiiri numbri telefoni juba ära salvestada. Küberturve elab omas hetkes ning see süsteem, mis täna töötab ja on turvaline, võib ilma hoolduseta juba aasta pärast auklik olla.

Eriti terav on see küsimus tarkvaraarenduste puhul. Toode näeb välja täpselt samasugune, olgu see turvaline või ebaturvaline. Kahjuks pole lõpptarbijale alati oluline, et tarkvara on arendatud nii, et kõik komponendid turvaliselt ja automaatselt uuenevad, kaasa tuleb logimise süsteem, mis teavitab kahtlastest tegevusest, sisselogimine on mitmeastmeline ning ebaseadusliku ligipääsu korral on riskid arvestatud ja maandatud.

Kui klientide andmed on varastatud, arvuti muutunud pahavaravõrgustiku osaks või vaatab ühel hommikul veebilehelt vastu Guy Fawkesi mask ja „h2cked by 1337 h4xx0r team“, siis imestatakse, kuidas see küll juhtus.

Eesmärk pole süüdistada ohvrit ega õigustada kurjategijat, vaid nentida, et pahatihti alahinnatakse küberriske. Rünnakute ärahoidmiseks ja hilisemaks politsei uurimiseks on kõik eelmainitud komponendid väga olulised.

### Eeltööst sõltub lõpptulemus

Küberrünnaku ohvriks võib langeda sõltumata infoturbe tasemest, kuid rünnaku ulatus sõltub sellest otseselt. Tänu heale eeltööle saab infoturbemeeskond kiiresti hinnata, kuidas omandati ligipääs süsteemidele, kui palju arvuteid kompromiteeriti, kas ja milliseid andmeid varastati. Samuti võimaldab see teha turvaanalüüsi ja hinnata, mida peab oma süsteemides muutma, et neid veelgi turvalisemaks teha. Selleks on vaja kompetentseid inimesi, kes teavad, millist infot oma süsteemidest koguda, et rünnakuid võimalikult kiiresti tuvastada. Isegi väga hea infoturbe puhul avastatakse osa ründeid mitu kuud hiljem, mistõttu tasub süsteemide logisid säilitada vähemalt aasta.

Logide olemasolu ja süsteemi dokumentatsioon muudab CERT-EE kaasamise oluliselt lihtsamaks ning tagab võimalused efektiivseks politseiuurimiseks. Kui süsteemi dokumentatsioon ja logid on olemas, saame meie kurjategija tuvastamise nimel juba suures osas iseseisvalt edasi tegutseda ning häirime infoturbe meeskonda kriisihetkedel minimaalselt.

Hea küberturbe tulemus on see, et kahju hinnatakse kiiresti, määratakse ja dokumenteeritakse rünnaku ulatus ning süsteemide töö taastatakse kiiresti. Vastupidisel juhul tekib suur segadus ja vastamine küsimusele „kas kurjategijal on endiselt meie süsteemide-

> Mida rohkem infot uurijad sündmuspaigalt saavad, seda tõenäolisem on kurjategija leida.

le ligipääs?“ on laias laastus loterii, kuna pole infot, mille pealt seda hinnata. Lisaks on süsteemide taastamine sellises olukorras frustreeriv ja võib osutuda väga kalliks.

Küberkuritegude puhul algab uurimine sündmuskohalt, täpselt samamoodi nagu kriminaalromaanides mõrva lahendamine. Mida rohkem infot uurijad sündmuspaigalt saavad, seda tõenäolisem on kurjategija leida. Küberkuritegu sarnaneb korterivargusega: seda on lihtne toime panna, kui uks on lukust lahti jäetud, aga meil on pärast väga keeruline juhtumit uurida, kui kannatanu on enne uurija saabumist kodu puhtaks küürinud.

# Eesti ja USA küberväed ühendasid jõud

Eesti ja Ameerika Ühendriikide küberväejuhatus (Cyber Command) viisid eelmise aasta septembrist novembrini Eesti kaitseväe võrgus läbi ühise küberoperatsiooni, mille eesmärk oli takistada pahatahtlike osapoolte sissepääsu võrku, tugevdada kahe riigi koostööd ja küberkaitsevõimeid.

USA küberspetsialistid, keda nimetatakse Hunt Forward meeskonnaks, ja Eesti küberväejuhatuse spetsialistid otsisid pahatahtlikke osapooli erinevates võrkudes ja platvormidel. USA on sarnaseid operatsioone Euroopas varasemalt läbi viinud teiste riikidega, koostöö Eesti küberekspertidega oli esmakordne.

## Eesmärk tagada küberturvalisus

„Ühised operatsioonid meie lähima liitlase USAga on vajalikud, et tagada meie teenuste küberturvalisus. Need annavad meie spetsialistidele võimaluse jagada kogemusi ning võimaldavad saada tagasisidet meie praeguse küberkaitsevõime kohta. Operatsioon oli edukas verstapost meie koostöös USA partneritega," ütles Eesti kaitseväe küberväejuhatuse ülema asetäitja Mihkel Tikk.

„Pandeemiale vaatamata saame tegutseda Eestis ja mujal Euroopas, mis annab meile võimaluse õppida vastaste kohta, kes võivad ohustada ka Ameerika Ühendriike," ütles brigaadikindral Joe Hartman, kes juhib Ameerika kübermissioonide keskust (Cyber National Mission Force).

Vastavad meeskonnad otsivad ja eemaldavad aktiivselt vastaspoolte pahavara. Seejärel jagavad nad teavet selle pahavara kohta mitte ainult USA valitsusega, vaid ka erasektori küberkaitseettevõtete ja liitlastega, et tõsta USA kriitilise taristu ja seotud võrkude turvalisust.

## Eesti riigikaitse sõltub küberist

USA Hunt Forward meeskonnad mängivad väga olulist rolli USA küberväejuhatuse Persistent Engagement initsiatiivis, mille eesmärk on takistada pahatahtlikku tegevust küberruumis, mis jääb allapoole otsese sõjategevuse piiri.

USA küberväejuhatuse ekspertide ülesanne on kaitsta USA valitsuse võrke ja platvorme vastaste eest. USA relvajõudude nn Defend Forward strateegia näeb ette koostööd oluliste partneritega, et ennetada küberruumis tegevusi, mida on võimalik kasutada ka USA kriitilise taristu vastu.

„Eesti digitaalne ühiskond sõltub küberist, samuti riigikaitse. Meie jaoks on oluline, et Eesti oli üks esimesi, kellega USA sellise ühisoperatsiooni läbi viis. See andis meile võimaluse saada hinnang meie võrkude turvalisuse kohta. Kuivõrd oleme maailmas liidrid küberteemadel, peame olema valmis kogemusi jagama ka liitlastega, et oma võrke paremini kaitsta," ütles Eesti kaitseministeeriumi asekantsler Margus Matt, kelle vastutusalasse kuulub ka küberpoliitika.

Küber on meeskonnasport – keegi ei suuda küberohte peatada üksinda!

### Küber on meeskonnasport

Potentsiaalseid ohte küberruumis hinnates annab selline partnerlus Eesti ja USA vahel võimaluse mõlemale riigile arendada enda küberkaitse võimeid, mis toetavad ka globaalset küberturvalisust. Pahavara tuvastamine ning selle kohta info jagamine avaliku ja erasektoriga tõstab kõikide kasutajate turvalisust küberruumis.

„Küber on meeskonnasport – keegi ei suuda küberohte peatada üksinda," ütles USA asekaitseminister küberpoliitika alal Thomas Wingfield. „Meie strateegia põhineb koostööl liitlastega ning partneritega erasektoris, akadeemias ja valitsustega, tagamaks, et meie küberruum on turvaline ja avatud mootor innovatsiooniks ning arenguks," lisas Wingfield. USA küberväejuhatus töötab koostöös USA Euroopa väejuhatuse ja NATO liitlastega ööpäev ringi, et takistada pahatahtlikku tegevust küberruumis.

Eesti ja USA kaitsealane küberkoostöö toimub mitmel tasandil USA küberväejuhatuse, USA Euroopa väejuhatuse, Marlyandi rahvuskaardi ja USA õhuväe küberväejuhatusega.

# Ciberseguridad: donde hay gana, hay maña*

RIA juhitav EU CyberNet rajab Dominikaani Vabariiki **küberturvalisuse oivakeskuse**, mis pakub tuge kõikidele Ladina-Ameerika riikidele.

Euroopa Liit on maailma suurim arenguabi andja. Üha suurem osa sellest abist toimub digiteerimise ja küberturvalisuse valdkonnas. EL on varemgi viinud läbi mitmeid küberturvalisuse projekte, kuid 2019. aasta septembris alustas Euroopa Komisjon neist värskeimaga – EU CyberNetiga, mille elluviija on RIA.

EU CyberNet

**Mis on EU CyberNeti eesmärk?**

EU CyberNeti eesmärk on koordineerida ELi poolt kolmandatele riikidele pakutavat abi nende küberturvalisuse tugevdamisel. Selle töö toetamiseks, aga ka ELi kübereksperdite kokku toomiseks, nende omavahelise koostöö ja professionaalsete oskuste parandamiseks moodustame võrgustiku, kuhu kuulub vähemalt 500 eksperti ning 150 asutust üle kogu Euroopa.

Olles vedanud projekti veidi üle aasta, saime 2020. aasta lõpus Brüsselist kaks olulist uudist ning tunnustust. Esiteks kirjutati EU CyberNeti keskne roll sisse uude ELi küberturvalisuse strateegiasse. Ja teiseks tegi Euroopa Komisjon meile ettepaneku pikendada projekti kaks aastat koos ülesandega viia selle tegevus uuele

## Ajajoon
### EU CyberNeti saamislugu

**2013**
- Euroopa Liidu küberjulgeoleku strateegia

**2014**
- Nõukogu järeldused arengukoostöö õigustepõhise, sh kõigi inimõiguste põhise käsitluse kohta

**2015**
- Euroopa julgeoleku tegevuskava
- Nõukogu järeldused küberdiplomaatia kohta

**2016**
- Ühtne visioon, ühine tegevus: tugevam Euroopa. Euroopa Liidu üldine välis- ja julgeolekupoliitika strateegia

**2017**
- Euroopa arengukonsensus
- Ühisteatis „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“

tasemele: võtta küberkoolitada kogu ELi välisesinduste võrgustik ja rajada Dominikaani Vabariigis alaline küberturvalisuse oivakeskus, mis kataks kogu Ladina-Ameerika.

### Miks Ladina-Ameerika?

Küberturvalisuse kontekstis muudavad Ladina-Ameerika ja Dominikaani Vabariigi ELi jaoks oluliseks partneriks nende ambitsioon viia ellu ühiskonna laiem digiteerimine ja saavutada kõrge valmidus küberintsidentidele vastamises, aga ka laiemad väärtused.

Ladina-Ameerika riikide üldisel hoiakul küberturbesse on veel küpsemisruumi ja riigiti on tase erinev. Neist vähestel on paigas reeglistik elutähtsa taristu küberkaitseks või tõhusalt toimiv partnerlus riigi ja erasektori vahel. Küberõppused on pigem harvad ja Euroopa Liidu või NATO-laadset integratsiooni kontinendi riikide vahel pole ette näha.

Lisades siia samal ajal õitseva IKT-sektori, on näha, et EU CyberNetil on tänu ekspertvõrgustikule ja praktilisele abile võimalik oluliselt kaasa aidata. Saame suurendada riikide teadlikkust küberturvalisusest, tihendada sidemeid valitsuste, akadeemilise ja erasektori vahel.

Suurema sidususe ja koostöö kaudu aitame kaasa, et ühegi Ladina-Ameerika riigi kriitiline infotaristu ei satuks vaenulike tegevuste ohvriks, sest sellest võib alguse saada ülemaailmse mõjuga küberintsident.

### Kuidas me seda teeme?

Rahvusvahelist ja regionaalset asutust ei raja üleöö. Õnneks on Eestil siin ette näidata unikaalne kogemus NATO küberkaitsekoostöö keskuse loomise ja arendamise näol.

Regionaalseid keskuseid tekib juurde. Nii näiteks on Singapur loonud oma pinnale sellise ASEANi riikide jaoks. Aafrikas on sarnaseid algatusi vähemalt kaks. Ladina-Ameerikas seni niisugust pole ning see seab ELile ja RIA-le vastutusrikka ülesande.

Keskus peaks saavutama esialgse tegutsemisvalmiduse 2021. aasta lõpuks. Sealjuures on meie eesmärk tekitada maksimaalselt sünergiaid EU CyberNeti algupäraste ülesannetega ehk rahvusvahelise ekspertvõrgustiku loomine ja koolituste korraldamine. Tahame näidata, et keerulisi asju on võimalik ellu viia ka kodust kaugel, kui on tahe, plaan ja pädevad inimesed.

> Tahame näidata, et keerulisi asju on võimalik ellu viia ka kodust kaugel.

Kui tead, kuidas näiteks ellu viia valdkondlikke ja/või riiklikke strateegiaid, suurendada institutsionaalset võimekust, kirjutada inimõigusi austavaid seadusi, kaitsta kriitilise informatsiooni infrastruktuuri, korraldada CERTi tööd või ehitada rahvusvahelisi koostöövõrgustikke – anna meile endast märku veebilehel www.eucybernet.eu/expert-pool. *Adelante!* **

* Küberturvalisus – kus on tahe, on võimalus (hispaania k)
** Edasi! (hispaania k)

**2018**
- ELi Nõukogu järeldused ELi-välise kübersuutlikkuse suurendamise suuniste kohta
- Tegevusjuhised ELi rahvusvahelise koostöö kohta kübersuutlikkuse suurendamiseks

**2019**
- Projekti EU CyberNet algus

**2020**
- Esimene eksperdilähetus
- Ekspertide ja kogukonna andmebaasi kasutuselevõtt

**2021**
- Rajame Dominikaani Vabariiki küberturvalisuse oivakeskuse

**2023**
- 500 eksperdist ja 150-liikmelisest kogukonnast koosnev võrgustik

# Eesti on küberdiplomaatia teerajaja

Küberkonfliktis karastunud riigina on Eesti rahvusvahelise poliitika üks põhisuundi olnud küberküsimused. Mida me selles vallas saavutanud oleme, kirjutab välisministeeriumi küberdiplomaatia osakonna peadirektor **Heli Tiirmaa-Klaar.**

2007. aastal, kui Eestit tabasid ulatuslikud küberrünnakud, polnud olemas ühtegi rahvusvahelist poliitilist mehhanismi, mille kaudu tõstatada küberrünnete olulisust, kutsuda appi teisi riike või mõista hukka ründajaid. Alates sellest ajast on Eesti teinud ära olulise töö küberjulgeoleku teema tõstatamisega nii rahvusvahelistes organisatsioonides kui ka kahe- ja mitmepoolses diplomaatias.

## Küberruumis kehtib rahvusvaheline õigus

Praegu leiame end sootuks erinevas kohas. Meil on olemas üleilmne küberstabiilsuse raa-

mistik, mis kinnitab üle rahvusvahelise õiguse kehtimise küberruumis ja sätestab riikidele käitumisreeglid.

See on sündinud viimase kümne aasta jooksul tänu ÜRO küberekspertide töörühmadele (UN Group of Governmental Experts). Kuuest korrast viiel on sellesse olulisse seltskonda valitud ka Eesti. Edaspidigi jääb ÜRO oluliseks paigaks, et aidata rakendada raamistikku, suurendada riikidevahelist usaldust ja kasvatada kübervastupanuvõimet, seda eriti arengumaades.

Küberdiplomaatide pinev töö võib väljast paista omaette nišina, mille kese on töörühmad, raportid ja konverentsid. Eesti jaoks on olnud oluline kasvatada ka laiemat arusaama küberteemadest rahvusvahelise julgeoleku kontekstis. Ainult nii saavad riigid teha teadlikke otsuseid.

### Mõistsime hukka küberründed Gruusia vastu

ÜRO Julgeolekunõukogu valitud liikmena 2021. aasta lõpuni on Eesti maailma kõige olulisemate diplomaatiliste arutelude absoluutses keskmes. Oleme kasutanud seda areenina, et tõsta küberteadlikkust veelgi laiema ringi seas. Märtsis 2020 tegi Eesti midagi ajaloolist: koos USA ja Ühendkuningriigiga mõistsime hukka mõni kuu varem toimunud ulatuslikud küberründed Gruusia vastu. See oli esimene kord, kui julgeolekunõukogu ametliku laua taga tõstatati konkreetsed küberründed.

Olime teerajajad ka mitteametliku virtuaalistungiga 22. mail 2020, mis keskendus küberruumi stabiilsusele ja konfliktiennetusele. Tugevalt jäi kõlama Eesti ja paljude teiste riikide veendumus, et küberruum ei erine muudest valdkondadest, kus kohaldatakse rahvusvahelist õigust ja riikidele kehtivad teatud käitumisreeglid. Kokku osales istungil ligikaudu 60 riiki ja organisatsiooni. Sel aastal on meil julgeolekunõukogus kavas astuda järgmine samm küberteemade teadlikkuse kasvatamiseks.


## Tallinna küberdiplomaatia suvekool

Küberdiplomaatia peavoolustamiseks välispoliitika osana ei piisa suurtest tähtsatest kohtumistest. Välisministeerium korraldab erinevaid koolitusi nii ELi ja NATO kui ka teiste kübervaldkonnas aktiivsete riikide diplomaatidele.

2019. aastal tegime algust ülipopulaarse Tallinna küberdiplomaatia suvekooliga ja nüüdseks oleme jõudnud paljude diplomaatideni maailmas. 2021. aasta veebruaris toimunud virtuaalne talvekool on kõigile järelevaatamiseks avatud välisministeeriumi kodulehel. vm.ee/et/node/53915

Eesti jaoks on olnud oluline kasvatada laiemat arusaama küberteemadest rahvusvahelise julgeoleku kontekstis.

# Euroopa Liit asutab küber-kompetentsi-keskuse

Euroopa Liit suurendab märkimisväärselt investeeringuid küberturbega seotud teadus- ja arendustegevusse. Selle käigus luuakse ELi küberkompetentsikeskus ja riiklike koordinatsioonikeskuste võrgustik.

Pärast pikki läbirääkimisi otsustasid Euroopa seadusandjad, et administratiivsete funktsioonidega ELi küberkompetentsikeskus (CCC) hakkab asuma Bukarestis. Lisaks sellele rajatakse riiklike koordinatsioonikeskuste (NCC) võrgustik, millest saab ELi peamine küberturbealase teadus- ja arendustegevuse vedaja. ELi määrusega luuakse ka pinnas korrapärasemaks koostööks ettevõtetega.

### Liikmesriigid saavad rohkem sõnaõigust

ELi järgmiseks mitmeaastaseks eelarveperioodiks (2021–2027) on loodud uus Digitaalse Euroopa programm (DEP), mille küberturvalisusele eraldatud 1,7 miljardit eurot hakkab haldama uus kompetentsikeskus. Samuti liiguvad Euroopa Horisondi rahastu küberturbe projektid uue keskuse koordineerida. Selline korraldus tähendab, et teadustöö praegusele tehnokraatlikule juhtimisele lisandub liikmesriikide suurem sõnaõigus prioriteetide seadmisel ning projektide kinnitamisel.

Lisaks teadlastele on uue võrgustiku kandvaks jõuks riiklikud koordinatsioonikeskused ehk NCCd, milleks iga liikmesriik nimetab ühe küberturbe võimekust omava asutuse või konsortsiumi. NCC-le on ette nähtud eraldi eelarve DEPist, mida tuleks kasutada määrusest tulenevate ülesannete täitmiseks, sealhulgas küberturbe teadus- ja arendusvõime kasvatamiseks. NCCd juhivad liikmesriikide vahelisi ühiseid tegevusi, kus eri riikide teadlased ja eksperdid arendavad konkreetseid küberturbe tehnoloogiaid või oskusi.

### Ettevõtete ja teadlaste kogukond

Kolmas oluline uuendus on ettevõtetest ja teadlastest loodav kogukond, mille liikmed koordineerivad teadus- ja arendustegevusi oma riigis ja ELi-üleselt ning ühtlasi annavad nad nõu CCC-le tööplaanide koostamisel.

> ELi uus küberturbe teadus- ja arendustöö raamistik saab tuule tiibadesse 2021. aasta teises pooles.

Kuigi ELi seadusandjad leidsid läbirääkimistel määruse suhtes kompromissi juba mullu detsembris, jõustus eelnõu tänavu märtsis. Igal liikmesriigil tuleb NCC määrata sellele järgneva kuue kuu jooksul, pärast seda võib alustada konkreetsete projektidega. Seega saab ELi uus küberturbe teadus- ja arendustöö raamistik tuule tiibadesse 2021. aasta teises pooles.

## Interreg CYBER soodustab koostööd küberturbe vallas

Euroopa Liit soodustab regionaaltasandi koostööd Interregi platvormi vahendusel, mille eesmärk on tõhustada piiriüleseid ühiseid algatusi ning aidata järele kontinendi vähemarenenud piirkondi. Küberturbe valdkonnas on niisugune koostööformaat uudne. Selleks loodi programm, mille eesmärk on parandada väikeste ja keskmise suurusega ettevõtete (VKE) konkurentsivõimet.

Eestit esindab 2023. aasta suveni kestvas Interreg CYBERi projektis RIA. Küberturbe alal tegutsevate VKEde võimekust arendatakse ökosüsteemide tugevuste ja puuduste väljaselgitamisel, parimate praktikate vahetamisel ning rakenduskavade ja tegevuste elluviimisel.

RIA sõelus teiste projektipartnerite praktikatest välja kaks, millest inspireeritud projekte on Eestis juba teostama hakatud: Britanniast tiivustatud „küber-hommikusöök“, mis on küberturbe ettevõtteid, ülikoole ja riigiameteid koondav regulaarne kohtumiste sari, ning vee-ettevõtete arenguprogramm, mis koostati arvestades soovitusi Sloveenia projektipartneritelt.

Samuti on projekti raames korraldatud küberturbe häkatone, mille kontekstis panustas RIA 2020. aasta detsembris toimunud „Küberpuuringu“ võistluse toimumisse.

# Euroopa Liit uuendab NIS direktiivi

Möödunud aasta detsembris avaldas Euroopa Komisjon ettepanekud **võrgu- ja infosüsteemide turbe** (NIS) direktiivi muutmiseks. Milliseid muudatusi need jõustumise korral kaasa tooks?

NIS direktiivi eesmärk on tõsta küberturvalisuse taset Euroopa Liidu riikides ja ühtlustada vastavaid seadusi. Kuna tase on riigiti väga erinev, nagu ka nägemused olukorra parandamise võimalustest ja vajalikkusest, seisavad ees pingelised läbirääkimised.

## Suurus määrab

Seni on kõige rohkem kõneainet pakkunud ettepanek laiendada NIS direktiivi kohaldamisala ja kehtestada nn suuruse reegel. See tähendab, et teatud valdkondade – muu hulgas toidu valmistamine, postiteenus ja jäätmekäitlus – 50 või enama töötajaga ettevõtted peaksid direktiivist juhinduma. Raamistikku on ettepanekus hõlmatud ka riigisektor.

Selle reegli rakendamisel kohalduksid uued nõuded sadadele tuhandetele Euroopas tegutsevatele ettevõtetele, Eestis lisanduks neid tõenäoliselt sadakond. Lisaks on igal riigil võimalik hõlmata mõned väiksemad kriitilise tähtsusega ettevõtted.

Mitme liikmesriigi pädevale asutusele näib tuhandete üksuste lisandumisega kaasnev koormuse kasv hoomamatu, seda eriti järelevalve tõttu.

## Astume ühte sammu

Komisjon on direktiiviga seadnud mitu läbivat eesmärki, millest üks on liikmesriikide küberturbe tagamise korralduse ühtlustamine. Seda üritatakse ette kirjutada detailsete nõuetega, mida tuleb strateegiate ja riiklike küberkriiside haldusraamistike koostamisel kindlasti arvestada.

Nende raamistike elluviimise tõhusust hindab ELi küberturbe amet ENISA, mis arvestab strateegia rakendamise mõõdikuid riikide küberturbe küpsuse indeksi koostamisel.

Samuti proovitakse tugevdada koostööd ja tõsta usaldust liikmesriikide vahel vastastikuste hindamistega, mida tehakse nii strateegilisel, operatiivsel kui tehnilisel tasandil. Komisjon esitas ka plaani luua ELi turvanõrkuste register, mis vastaks ELi vajadustele ja

eripäradele ning täiendaks USA haavatavuste andmebaasi (NVD).

### Küberturbe eest vastutab juhtkond

Võrreldes kehtiva direktiiviga on uus ettepanek turvanõuete suhtes palju detailsem. Kõik, kel tuleb direktiivist juhinduda, peaksid koostama konkreetsed eeskirjad nii tarneahela turvalisuse, üldise infoturbe korra kui ka krüptograafia kasutamise kohta.

Samuti on lähtutud põhimõttest, et küberturbe meetmete eest vastutab ettevõttes peamiselt juhtkond ning neid on nõuete mitte täitmise eest võimalik vastutusele võtta. Põhimõte on muutunud ka järelevalve reeglites ja trahvide suuruses, kus rikkumiste puhul määratavad summad sarnanevad andmekaitse üldmääruse omadega.

## Teekond NIS 2.0ni

- 2016. aastal jõustus võrgu- ja infosüsteemide turbe direktiiv (NIS), milles eesmärk on parandada küberturvalisuse taset Euroopa Liidu liikmesriikides.
- 2020. aasta detsembris avaldas Euroopa Komisjon ettepanekud NIS direktiivi muutmiseks.
- NIS 2.0 põhilised muudatused puudutavad direktiivi kohaldamisala, teabevahetust, turvanõudeid ja trahvimäärasid direktiivi nõuete rikkumise eest.
- NIS 2.0 võtavad ELi seadusandjad vastu tõenäoliselt kahe aasta jooksul, misjärel on liikmesriikidel 18 kuud selle kohaldamiseks oma riigi õigusaktidesse.

Võrreldes kehtiva direktiiviga on uus ettepanek turvanõuete suhtes palju detailsem.

# Küberturvalisuse aastaraamat 2021

Väljaandja: **Riigi Infosüsteemi Amet**
Pärnu mnt 139a, 11317 Tallinn

Kujundus: **Martin Mileiko** (Profimeedia OÜ)

Illustratsioonid: **Tolm OÜ** ja
**Linda Vainomäe** (Profimeedia OÜ)

Foto: **Nelli Pello**

Trükk: Ecoprint AS

Loe edasi: **www.ria.ee**